BELKIN

ADSL2+ Modem with Wireless G+ MIMO Router

Network your computers and share your ADSL Internet access

UK
FR
DE
NL
ES
IT



802.11g
G+
MIMO

User Manual

F5D9630uk4A

Table of Contents

Thank you for purchasing the Belkin ADSL Modem with High-Speed Mode Wireless G Router (the Router). In minutes you will be able to share your Internet connection and network your computers with your new Router. The following is a list of features that make your Router an ideal solution for your home or small office network. Please be sure to read through this User Manual completely, and pay special attention to Appendix B entitled "Important Factors for Placement and Setup".

Benefits of a Home Network

By following our simple setup instructions, you will be able to use your Belkin home network to:

- Share one high-speed Internet connection with all the computers in your home
- Share resources, such as files, and hard drives among all the connected computers in your home
- Share a single printer with the entire family
- Share documents, music, video, and digital pictures
- Store, retrieve, and copy files from one computer to another
- Simultaneously play games online, check Internet email, and chat

Advantages of a Belkin Wireless Network

Mobility – you'll no longer need a dedicated "computer room"— now you can work on a networked laptop or desktop computer anywhere within your wireless range

Easy installation – Belkin's Easy Installation Wizard makes setup simple

Flexibility – set up and access printers, computers, and other networking devices from anywhere in your home

Easy Expansion – the wide range of Belkin networking products let you expand your network to include devices such as printers and gaming consoles

No cabling required – you can spare the expense and hassle of retrofitting Ethernet cabling throughout the home or office

Widespread industry acceptance – choose from a wide range of interoperable networking products

Make Sure You Have the Following

Package Contents

- ADSL2+ Modem with Wireless G+ MIMO Router
- RJ11 Telephone Cord - Gray
- RJ45 Ethernet Networking Cable - Yellow
- ADSL Microfilter*
- Power Adapter
- User Manual CD

*ADSL microfilter varies by country. If it's not included, you will need to purchase one.

System Requirements

- An active ADSL service with a telephone wall jack for connecting the Router
- At least one computer with a Network Interface Card (NIC) and Internet browser installed and correctly configured
- TCP/IP networking protocol installed on each computer connected to the Router
- No other DHCP server on your local network assigning IP addresses to computers and devices

Internet Connection Settings

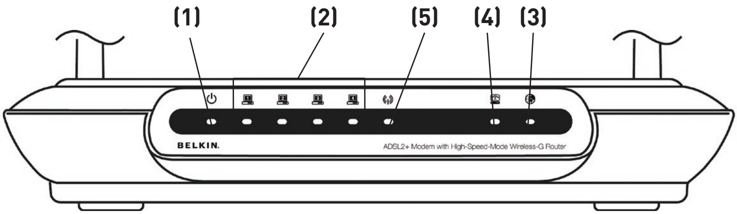
Please collect the following information from your Internet Service Provider (ISP) before setting up the ADSL Modem Wireless G Router.

- Internet connection protocol: ________ (PPPoE, PPPoA, Dynamic IP, Static IP)
- Multiplexing method or Encapsulation: _________ (LLC or VC MUX)
- Virtual circuit: VPI (Virtual Path Identifier) _________ (a number between 0 and 255)
- VCI (Virtual Channel Identifier) _________ (a number between 1 and 65535)
- For PPPoE and PPPoA users: ADSL account user name ____________ and password ______________
- For static IP users: IP Address ___ . ___ . ___ . ___
  Subnet Mask ___ . ___ . ___ . ___
  Default Gateway Server ___ . ___ . ___ .
- IP address for Domain Name Server ___ . ___ . ___ . ___ (If given by your ISP)

Note: See Appendix C in this User Manual for some common DSL Internet setting parameters. If you are not sure, please contact your ISP.

The Router is designed to be placed on a desktop. All of the cables exit from the rear of the Router for better organization and utility. The LED indicators are easily visible on the front of the Router to provide you with information about network activity and status.

Front Panel



1. **Power LED**
When you apply power to the Router or restart it, a short period of time elapses while the Router boots up. When the Router has completely booted up, the Power LED becomes a GREEN light, indicating the Router is ready for use.

	OFF	Router is OFF
	Green	Router is ON
	Red	Router failed to start

2. **LAN Status LEDs**
These LAN Status LEDs are labeled 1–4 and correspond to the numbered ports on the rear of the Router. When a computer is properly connected to one of the LAN ports on the rear of the Router, the LED will light. Solid GREEN means a computer or a network-enabled device is connected. When information is being sent over the port, the LED blinks rapidly. ORANGE indicates a 10Base-T connection.

	OFF	No device is connected
	Orange	Ethernet link is up and 10Base-T device connected
	Orange - blinking	When 10Base-T device transmitting or receiving data
	Green	Ethernet link is up and 100Base-T connected
	Green - blinking	When 100Base-T device transmitting or receiving data

3. WLAN Status LED

The WLAN Status LED is solid GREEN when you enable the wireless LAN function. It flashes when the Router is transmitting or receiving data wirelessly.

OFF	WLAN is off
Green	WLAN is up and connected
Green - blinking	When transmitting or receiving data

4. ADSL LED

The ADSL LED flashes GREEN during negotiation with your ISP. It stays GREEN when the Router is connected properly to your ADSL service.

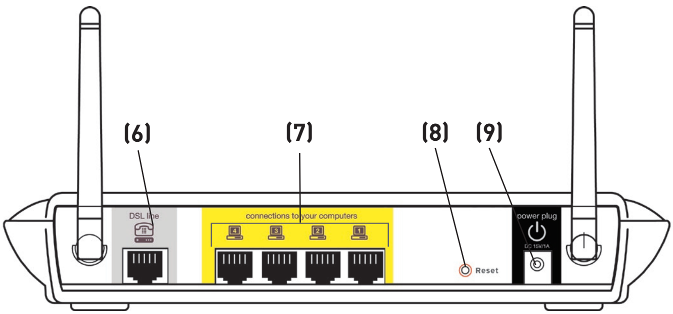
OFF	No ADSL connection
Green	ADSL link is up and connected
Green - blinking	negotiating connection

5. Internet LED

The Internet LED shows you when the Router is connected to the Internet. When the LED is OFF, the Router is NOT connected to the Internet. When the LED is solid GREEN, the Router is connected to the Internet. When the LED is blinking, the Router is transmitting or receiving data from the Internet.

OFF	No Internet connection
Green	Connected to the Internet
Green - blinking	When transmitting or receiving data
Red	Failed to get IP

Back Panel



6. **DSL Line**
   This port is for connection to your ADSL line. Connect your ADSL line to this port.

7. **Ethernet Ports**
   The Ethernet ports are RJ45, 10/100 auto-negotiation. The ports are labeled 1 through 4. These ports correspond to the numbered LEDs on the front of the Router. Connect your network-enabled computers or any networking devices to one of these ports.

8. **Reset Button**
   The "Reset" button is used in rare cases when the Router may function improperly. Resetting the Router will restore the Router's normal operation while maintaining the programmed settings. You can also restore the factory default settings by using the Reset button. Use the restore option in instances where you may have forgotten your custom password.

   a. **Resetting the Router**
      Push and hold the Reset button for one second then release it. When the Power/Ready light becomes solid again, the reset is complete.

   b. **Restoring the Factory Defaults**
      Press and hold the Reset button for five seconds then release it. When the Power/Ready light becomes solid again, the restore is complete.

9. **Power Plug**
   Connect the included 15V DC power supply to this inlet. Using the wrong type of power adapter may cause damage to your Router.

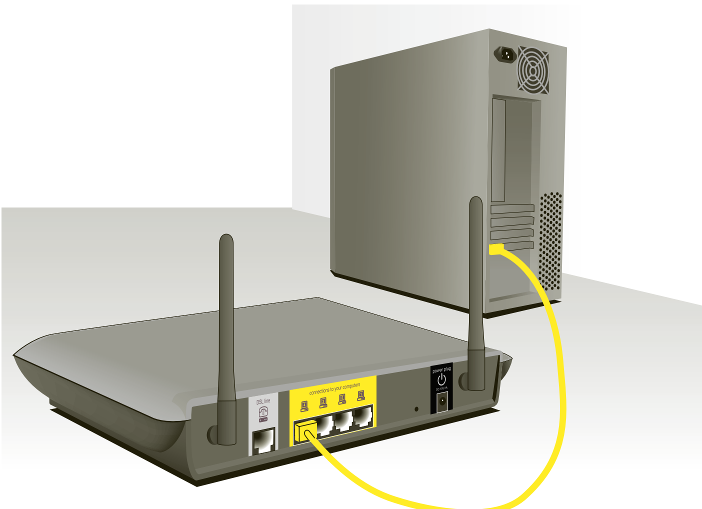
Positioning your Router

Your wireless connection will be stronger the closer your computer is to your Router. Typical indoor operating range for your wireless devices is between 100 and 200 feet. In the same way, your wireless connection and performance will degrade somewhat as the distance between your Router connected devices increases. This may or may not be noticeable to you. As you move farther from your Router, connection speed may decrease. Factors that can weaken signals simply by getting in the way of your network's radio waves are metal appliances, or obstructions, and walls. Please see "Appendix B: Important Factors for Placement and Setup" in this User Manual for more guidelines.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between five and 10 feet from the Router, in order to see if distance is the problem. If difficulties persist even at close range, please see the Troubleshooting section for solutions.

Connecting your Computers

1. Power off your computers and networking equipment.
2. Connect your computer to one of the YELLOW RJ45 ports on the rear of the Router labeled "connections to your computers" by using an Ethernet networking cable (one Ethernet network cable is supplied).

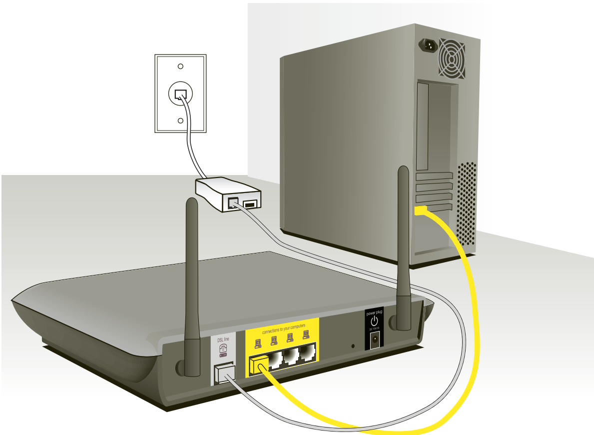


Connecting your ADSL Line

Connection for the Router to the ADSL line varies by country and region. Typically it involves a microfilter or a microfilter with built-in splitter to allow simultaneous use of ADSL service and telephone service on the same telephone line. Please read the following steps carefully and select appropriate method.

1. If your telephone service and ADSL service are on the same telephone line, ADSL microfilters are needed for each telephone and device, such as answering machine, fax machine, and caller ID display. Additional splitters may be used to separate telephone lines for telephone and the Router.

   Note: Do not connect the ADSL microfilter between the wall jack and the Router—this will prevent ADSL service from reaching the modem.
2. If your telephone service and ADSL service are on the same telephone line and you are using an ADSL microfilter with built-in splitter, connect the splitter to the telephone wall jack providing ADSL service. Then, connect the telephone cord from the ADSL microfilter RJ11 port generally labeled “DSL” to the gray RJ11 port labeled “DSL line” on the back of your Router. Connect telephony device to the other port on the ADSL splitter commonly labeled “Phone”. An additional ADSL microfilter is needed for another telephone and device on the same line.



Note: One RJ11 telephone cord is supplied. When inserting an RJ11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

3. If you have a dedicated ADSL service telephone line with an RJ11 wall jack, simply connect a telephone cord from the wall jack to the gray RJ11 port labeled “DSL line” on the back of your Router.

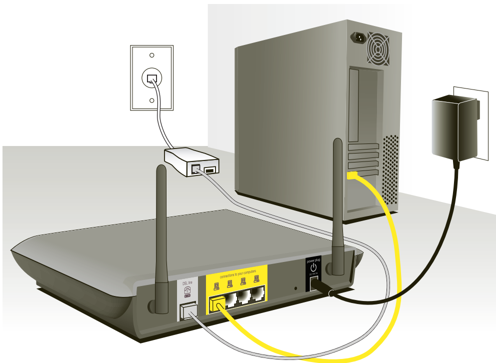
4. If you have an RJ45 wall jack for your ADSL service, connect an RJ45-to-RJ11 converter to the wall jack. Then connect one end of a telephone cord to the converter and the other end to the gray RJ11 port labeled “DSL line” on the back of your Router.

   Note: ADSL microfilter may or may not be provided depending on your country.

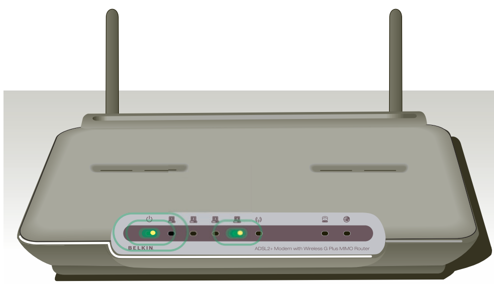
Powering Up your Router

1. Connect the supplied power adapter to the Router power-input plug labeled "Power".

   Note: For safety and performance reasons, only use the supplied power adapter to prevent damage to the Router.



2. After connecting the power adapter and the power source is turned on, the Router's power icon. ⏻ on the front panel should be on. It might take a few minutes for the Router to fully start up.



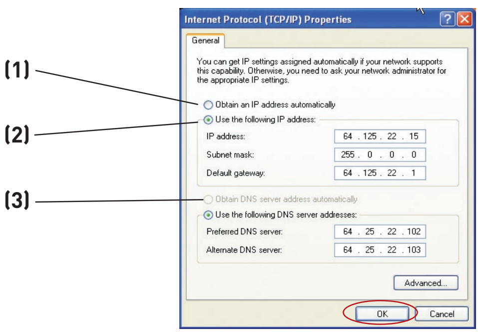
3. Turn on your computers. After your computers boot up, the LAN status LED 💻 on the front of the Router will be on for each port to which a wired computer is connected. These lights show you the connection and activity status. Now you are ready to configure the Router for ADSL connection.

In order for your computer to properly communicate with your Router, you will need to change your computer's "TCP/IP Ethernet" settings to "Obtain an IP address automatically/Using DHCP". This is normally the default setting in most home computers.

You can set up the computer that is connected to the ADSL modem FIRST using these steps. You can also use these steps to add computers to your Router after the Router has been set up to connect to the Internet.

Manually Configuring Network Adapters in Windows XP, 2000, or NT

1. Click "Start", "Settings", then "Control Panel".
2. Double-click on the "Network and dial-up connections" icon (Windows 2000) or the "Network" icon (Windows XP).
3. Right-click on the "Local Area Connection" associated with your network adapter and select "Properties" from the drop-down menu.
4. In the "Local Area Connection Properties" window, click "Internet Protocol (TCP/IP)" and click the "Properties" button. The following screen will appear:



5. If "Use the following IP address" **(2)** is selected, your Router will need to be set up for a static IP connection type. Write the address information the table below. You will need to enter this information into the Router.

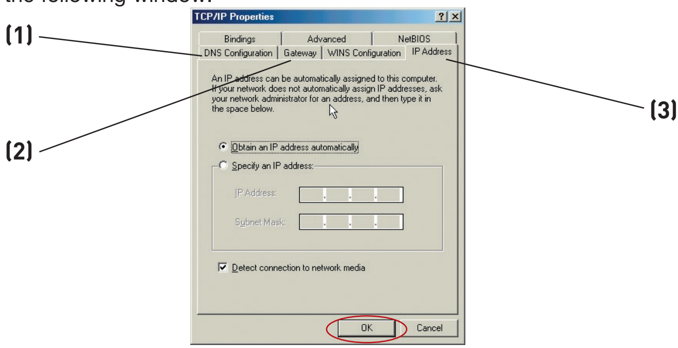
IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

6. If not already selected, select "Obtain an IP address automatically" **(1)** and "Obtain DNS server address automatically" **(3)**. Click "OK".

Your network adapter(s) are now configured for use with the Router.

Manually Configuring Network Adapters in Windows 98SE or Me

1. Right-click on "My Network Neighborhood" and select "Properties" from the drop-down menu.
2. Select "TCP/IP -> settings" for your installed network adapter. You will see the following window.



3. If "Specify an IP address" is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

4. Write the IP address and subnet mask from the "IP Address" tab **(3)**.
5. Click the "Gateway" tab **(2)**. Write the gateway address down in the chart.
6. Click the "DNS Configuration" tab **(1)**. Write the DNS address(es) in the chart.
7. If not already selected, select "Obtain an IP address automatically" on the IP address tab. Click "OK".
8. You will also need to delete the Gateway address from the Gateway tab and DNS Configuration entries in order to properly be configured for connection to the Belkin router.

Restart the computer. When the computer restarts, your network adapter(s) are now configured for use with the Router.

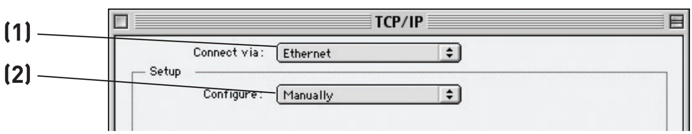
Set up the computer that is connected to the cable or DSL modem by FIRST using these steps. You can also use these steps to add computers to your Router after the Router has been set up to connect to the Internet.

Manually Configuring Network Adapters in Mac OS up to 9.x

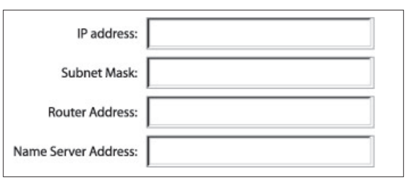
In order for your computer to properly communicate with your Router, you will need to change your Mac computer's TCP/IP settings to DHCP.

1. Pull down the Apple menu. Select "Control Panels" and select "TCP/IP".

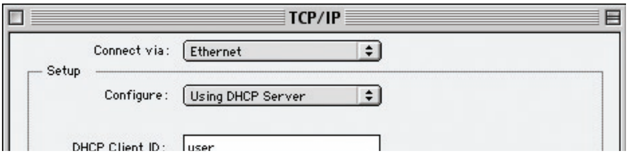
2. You will see the TCP/IP control panel. Select "Ethernet Built-In" or "Ethernet" in the "Connect via:" drop-down menu **(1)**.



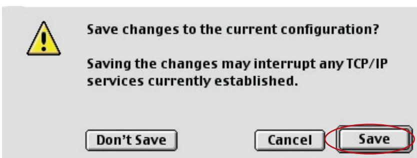
3. Next to "Configure" **(2)**, if "Manually" is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.



4. If not already set, at “Configure:”, choose “Using DHCP Server”. This will tell the computer to obtain an IP address from the Router.



5. Close the window. If you made any changes, the following window will appear. Click “Save”.



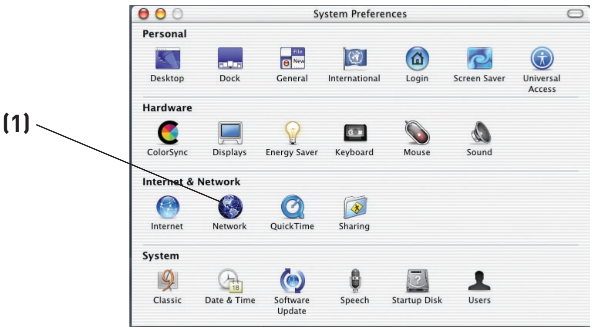
Restart the computer. When the computer restarts, your network settings are now configured for use with the Router.

Manually Configuring Network Adapters in Mac OS X

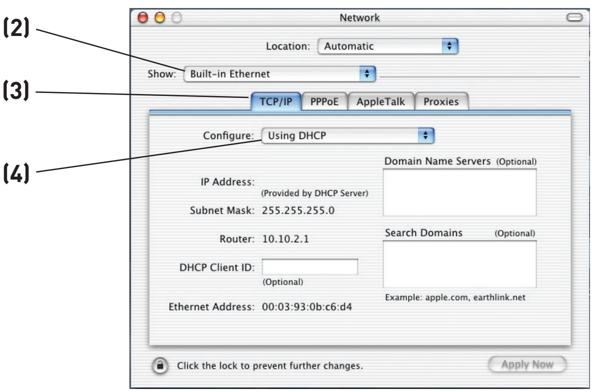
1. Click on the "System Preferences" icon.



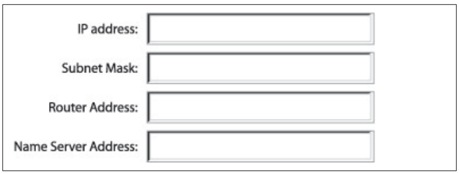
2. Select "Network" **(1)** from the "System Preferences" menu.



3. Select "Built-in Ethernet" **(2)** next to "Show" in the Network menu.



4. Select the “TCP/IP” tab **(3)**. Next to “Configure” **(4)**, you should see “Manually” or “Using DHCP”. If you do not, check the PPPoE tab **(5)** to make sure that “Connect using PPPoE” is NOT selected. If it is, you will need to configure your Router for a PPPoE connection type using your user name and password.
5. If “Manually” is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

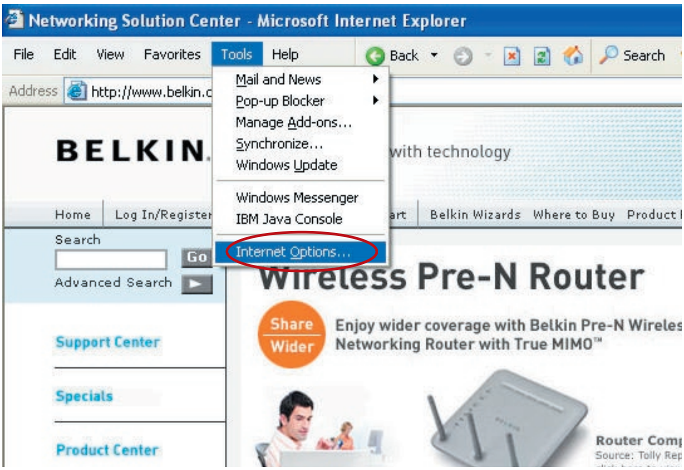


6. If not already selected, select “Using DHCP” next to “Configure” **(4)**, then click “Apply Now”.

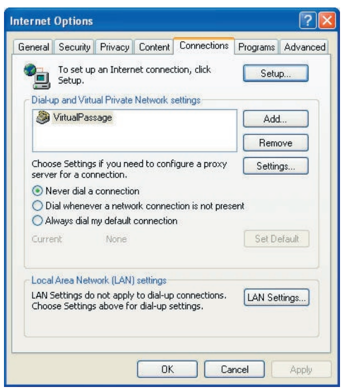
Your network adapter(s) are now configured for use with the Router.

Recommended Web Browser Settings

In most cases, you will not need to make any changes to your web browser's settings. If you are having trouble accessing the Internet or the advanced web-based user interface, then change your browser's settings to the recommended settings in this section.

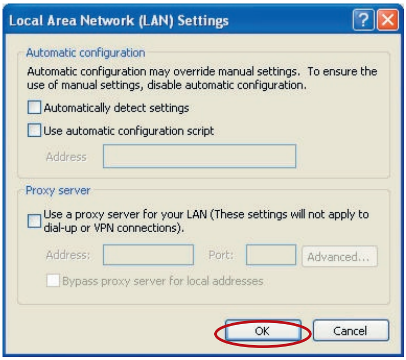


Internet Explorer 4.0 or Higher



1. Start your web browser. Select "Tools" then "Internet Options".
2. In the "Internet Options" screen, there are three selections: "Never dial a connection", "Dial whenever a network connection is not present", and "Always dial my default connection". If you can make a selection, select "Never dial a connection". If you cannot make a selection, go to the next step.
3. Under the "Internet Options" screen, click on "Connections" and select "LAN Settings…".

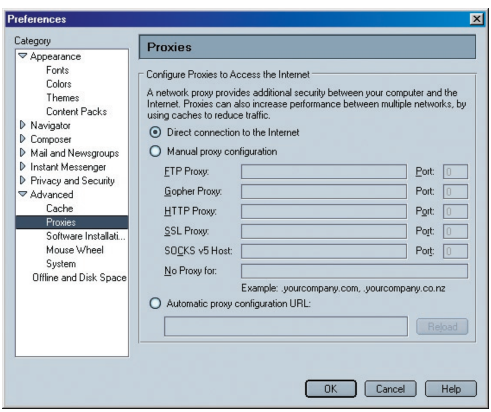
4. Make sure there are no check marks next to any of the displayed options: "Automatically detect settings", "Use automatic configuration script", and "Use a proxy server". Click "OK". Then click "OK" again in the "Internet Options" page.



Netscape Navigator 4.0 or Higher

1. Start Netscape. Click on "Edit" then "Preferences".

2. In the "Preferences" window, click on "Advanced" then select "Proxies". In the "Proxies" window, select "Direct connection to the Internet".



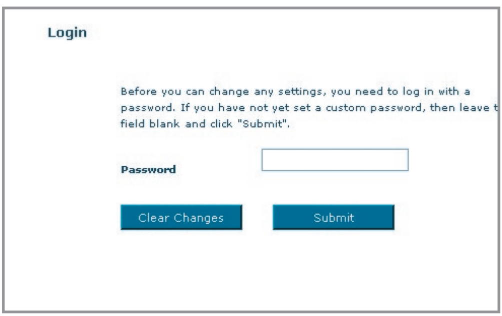
Running the Setup Wizard

1. You can access the web-based management user interface of the Router using the Internet browser on a computer connected to the Router. Type "192.168.2.1" (do not type in anything else such as "http://" or "www") in your browser's address bar. Then press the "Enter" key.



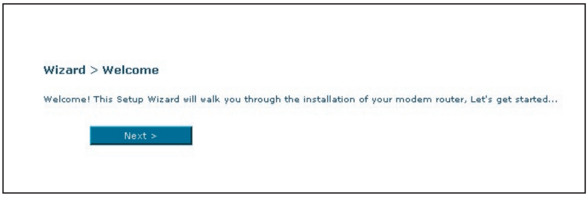
Note: It is strongly recommended that you use a computer physically connected to the Router with an RJ45 cable for initial setup. Using a wirelessly connected computer for initial setup is not recommended.

2. The following screen will appear in your browser to prompt you to login. The Router ships with no password entered. In the login screen, leave the password blank and click the "Submit" button to log in.

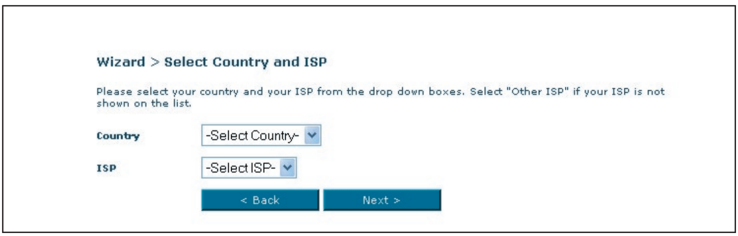


Note: It is strongly recommended that you change the password to your own for increased security. Please read the following section, entitled "Manually Configuring your Router", for details on how to change your password and to reference other security features.

3. The Setup Wizard will start automatically for express configuration (recommended) Click "Next" to continue.



4. The first step is to select your country and ISP, and click "Next". If your country and/or ISP is not listed, select "Other Country" or "Other ISP."



5. Now fill in the username and password you were supplied by your Internet Service Provider (ISP) in to the blank fields. It is important that the correct user name and password are entered otherwise the connection will fail. Your ISP will be able to confirm your user name and password.



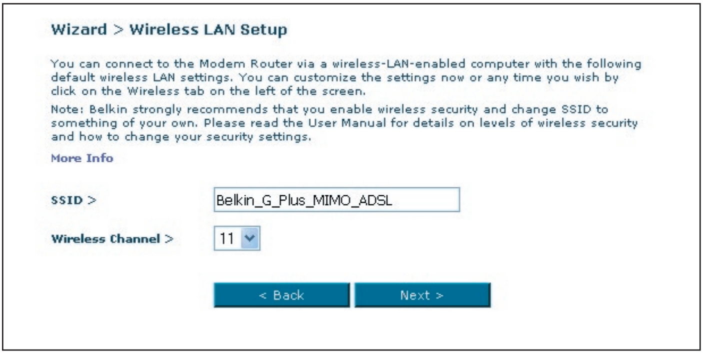
Note: For more detailed instruction on other connection types, please refer to the "Manually Configuring your Router" section of this User Manual.

6. Now the Wireless LAN Setup screen will show. You can connect to the Router via a wireless-LAN-enabled computer with the following default wireless LAN settings:

   SSID = Belkin G+ MIMO ADSL

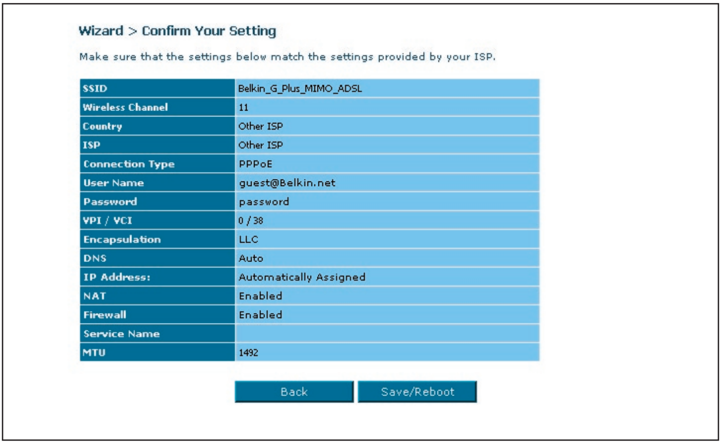
   Wireless Channel = Auto

   Security = off



Note: Belkin strongly recommends that you enable wireless security to WEP or WPA and change SSID to something of your own. Please read the User Manual for details on levels of wireless security and how to change your security settings

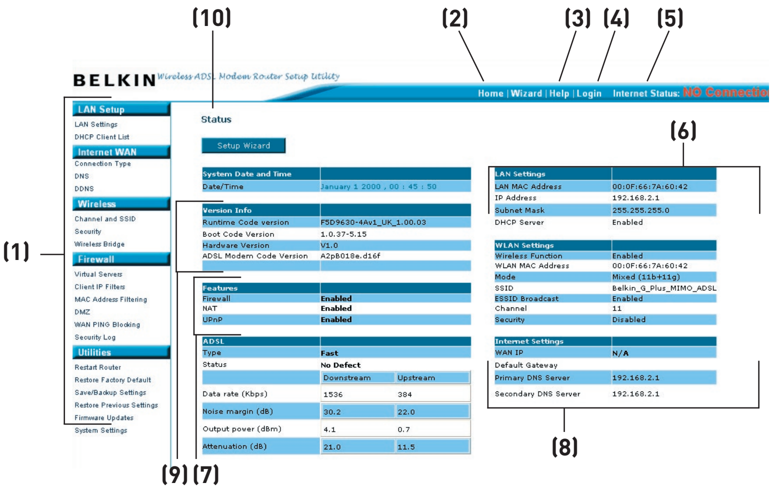
7. Double-check the settings shown on the following screen. You can click “Back” to change the settings or click “Next” to confirm



Note: You can always restart the Setup Wizard or use the Navigation Menu on the left to change your setting.

Understanding the Web-Based User Interface

The home page shows you a quick view of the Router's status and settings. All advanced setup pages can be reached from this page.



1. **Quick-Navigation Links**
   You can go directly to any of the Router's UI pages by clicking directly on these links. The links are divided into logical categories and grouped by tabs to make finding a particular setting easier to find. Clicking on the header of each tab will show you a short description of the tab's function.

2. **Home Button**
   The "Home" button is available in every page of the UI. Pressing this button will take you back to the home page.

3. **Help Button**
   The "Help" button gives you access to the Router's help pages. Help is also available on many pages by clicking "more info" next to certain sections of each page.

4. **Login/Logout Button**
   This button enables you to log in and out of the Router with the press of one button. When you are logged into the Router, this button will change to read "Logout". Logging into the Router will

take you to a separate login page where you will need to enter a password. When you are logged into the Router, you can make changes to the settings. When you are finished making changes, you can log out of the Router by clicking the “Logout” button. For more information about logging into the Router, see the section called “Logging into the Router”.

5. **Internet Status Indicator**

   This indicator is visible in all pages of the Router, showing the connection status of the Router. When the indicator says “connection OK” in GREEN, the Router is connected to the Internet. When the Router is not connected to the Internet, the indicator will read “no connection” in RED. The indicator is automatically updated when you make changes to the settings of the Router.

6. **LAN Settings**

   Shows you the settings of the Local Area Network (LAN) side of the Router. Changes can be made to the settings by clicking the “LAN” “Quick Navigation” link on the left side of the screen.

7. **Features**

   Shows the status of the Router’s UPnP, NAT, and firewall features. Changes can be made to the settings by clicking on any one of the links or by clicking the “Quick Navigation” links on the left side of the screen.

8. **Internet Settings**

   Shows the settings of the Internet/WAN side of the Router that connects to the Internet. Changes to any of these settings can be made by clicking on the “Internet/WAN” “Quick Navigation” link on the left side of the screen.

9. **Version Info**

   Shows the firmware version, boot-code version, hardware version, and serial number of the Router.

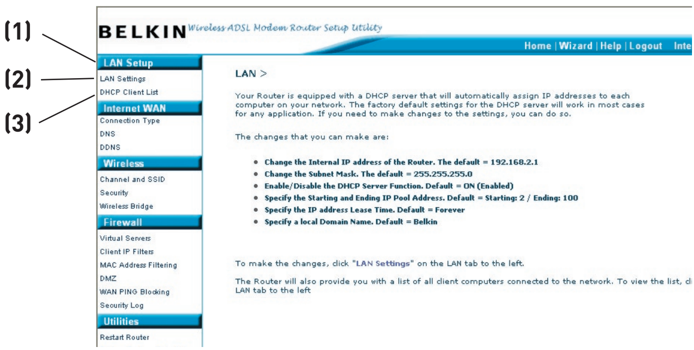
10. **Page Name**

    The page you are on can be identified by this name. This manual will sometimes refer to pages by name. For instance, “LAN > LAN Settings” refers to the “LAN Settings” page.

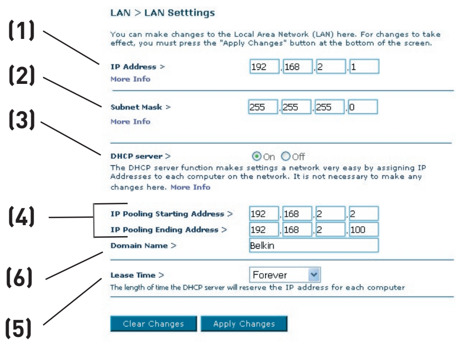
Changing LAN Settings

All settings for the internal LAN setup of the Router can be viewed and changed here.

Clicking on the header of the LAN tab **(1)** will take you to the LAN tab's header page. A quick description of the functions can be found here. To view the settings or make changes to any of the LAN settings, click on "LAN Settings" **(2)** or to view the list of connected computers, click on "DHCP Client List" **(3)**.



LAN Settings



1. **IP Address**

   The "IP address" is the internal IP address of the Router. The default IP address is "192.168.2.1". To access the setup interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type in the new IP address and click "Apply Changes". The IP address you choose should be a non-routable IP. Examples of a non-routable IP are:

   192.168.x.x (where x is anything between 0 and 255)

   10.x.x.x (where x is anything between 0 and 255)

2. **Subnet Mask**

   There is no need to change the subnet mask as the router will automatically adjust the length based on the IP address type.

3. **DHCP Server**

   The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network automatically. The default setting is "On". The DHCP server can be turned OFF if necessary, however, in order to do so you must manually set a static IP address for each computer on your network. To turn off the DHCP server, select "Off" and click "Apply Changes".

4. **IP Pool**

   The IP Pool is the range of IP addresses set aside for dynamic assignment to the computers on your network. The default is

2–100 (99 computers). If you want to change this number, you can do so by entering a new starting and ending IP address and clicking on "Apply Changes". The DHCP server can assign 100 IP addresses automatically. This means that you cannot specify an IP address pool larger than 100 computers. For example, starting at 50 means you have to end at 150 or lower so as not to exceed the 100-client limit. The starting IP address must be lower in number than the ending IP address.

5. **Lease Time**

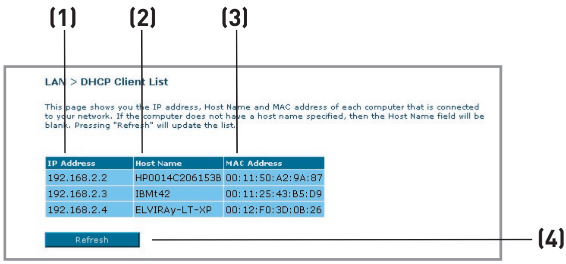
   Lease time is the length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to "Forever". The default setting is "Forever", meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular computer. Setting lease times for shorter intervals, such as one day or one hour, frees IP addresses after the specified period of time. This also means that a particular computer's IP address may change over time. If you have set any of the other advanced features of the Router, such as DMZ or client IP filters, these are dependent on the IP address. For this reason, you will not want the IP address to change.

6. **Local Domain Name**

   The default setting is "Belkin". You can set a local domain name (network name) for your network. There is no need to change this setting unless you have a specific advanced need to do so. You can name the network anything you want such as "MY NETWORK".

DHCP Client List

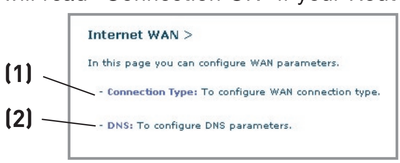
You can view a list of the computers (known as clients), which are connected to your network. You are able to view the IP address **(1)** of the computer, the host name **(2)** (if the computer has been assigned one), and the MAC address **(3)** of the computer's Network Interface Card (NIC). Pressing the "Refresh" **(4)** button will update the list. If there have been any changes, the list will be updated.



Internet WAN

The "Internet WAN" tab is where you will set up your Router to connect to your Internet Service Provider. The Router is capable of connecting to virtually any ADSL Service Provider's system provided you have correctly configured the Router's settings for your ISP's connection type. Your connection settings are provided to you by your ISP. To configure the Router with the settings that your ISP gave you, click "Connection Type" **(1)** on the left side of the screen. Select the connection type you use. If your ISP gave you DNS settings, clicking "DNS" **(2)** allows you to enter DNS address entries for ISPs that require specific settings.

When you have finished making settings, the "Internet Status" indicator will read "Connection OK" if your Router is set up properly.



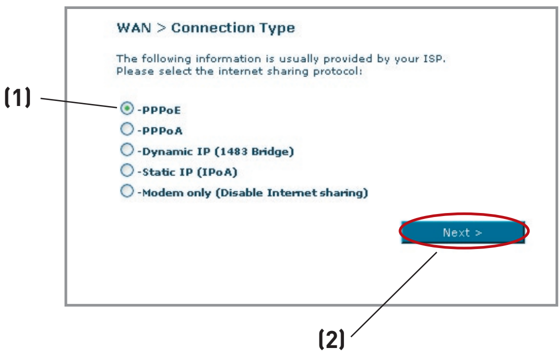
Connection Type

From the "Connection Type" page, you can select one of these five connection types based on the instruction provided by your ISP:

- PPPoE
- PPPoA
- Dynamic IP (1483 Bridged)
- Static IP (IPOA)
- Modem Only (Disable Internet Sharing)

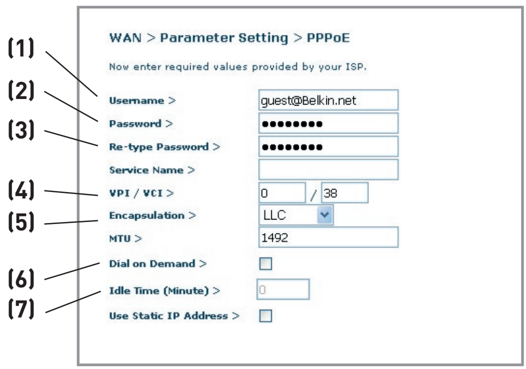
Note: See Appendix C in this User Manual for some common DSL Internet setting parameters. If you are not sure, please contact your ISP.

Select the type of connection you use by clicking the radio button **(1)** next to your connection type and then clicking "Next" **(2)**.



Setting your ISP Connection Type to PPPoE or PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) is the standard method of connecting networked devices. It requires a user name and password to access the network of your ISP for connecting to the Internet. PPPoA (PPP over ATM) is similar to PPPoE, but is mostly implemented in the UK. Select PPPoE or PPPoA and click “Next”. Then enter the information provided by your ISP, and click “Apply Changes” to activate your settings.



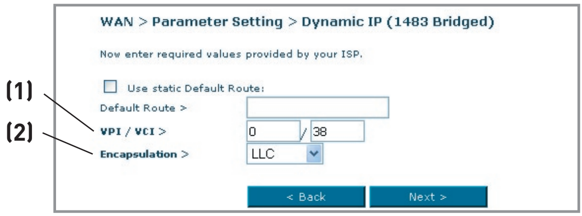
1. **User Name -** Enter the user name. (Assigned by your ISP).
2. **Password -** Enter your password. (Assigned by your ISP).
3. **Retype Password -** Confirm the password. (Assigned by your ISP).
4. **VPI/VCI -** Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).
5. **Encapsulation -** Select your encapsulation type (supplied by your ISP) to specify how to handle multiple protocols at the ATM transport layer.

   VC-MUX: PPPoA Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with fewer overheads.

   LLC: PPPoA Logical Link Control allows multiple protocols running over one virtual circuit (more overhead).
6. **Dial on Demand -** By selecting “Dial on Demand” your Router will automatically connect to the Internet when a user opens up a web browser.
7. **Idle Time (Minutes) -** Enter the maximum idle time for the Internet connection. After this time has been exceeded, the connection will be terminated.

Setting your Connection Type to Dynamic IP (1483 Bridged)

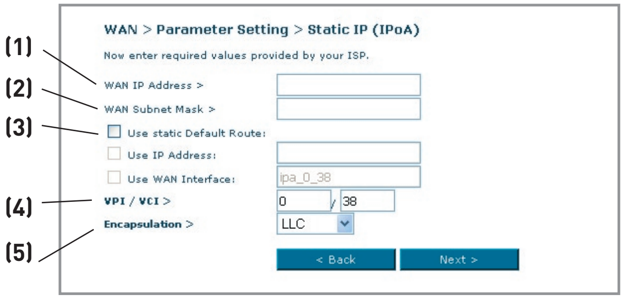
This connection method bridges your network and ISP's network together. The Router will obtain an IP address automatically from your ISP's DHCP server.



1. **VPI/VCI -** Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. These identifiers are assigned by your ISP.
2. **Encapsulation -** Select LLC or VC MUX your ISP uses.

Setting your ISP Connection to Static IP (IPoA)

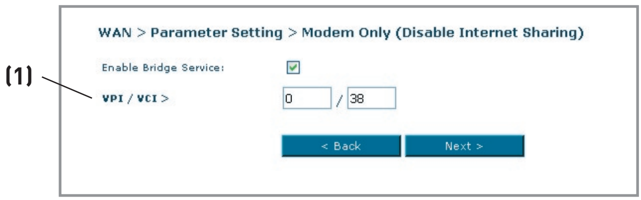
This connection type is also called "Classical IP over ATM" or "CLIP", which your ISP provides a fixed IP for your Router to connect to the Internet.



1. **WAN IP Address –** Enter an IP address assigned by your ISP for the Router WAN interface.
2. **WAN Subnet Mask -** Enter a subnet mask assigned by your ISP.
3. **Default Route -** Enter a default gateway IP address. If the Router cannot find the destination address within its local network, it will forward the packets to the default gateway assigned by your ISP.
4. **VPI/VCI -** Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. These identifiers are assigned by your ISP.
5. **Encapsulation -** Select LLC or VC MUX your ISP uses.

Setting your Connection Type to Modem Only (Disable Internet Sharing)

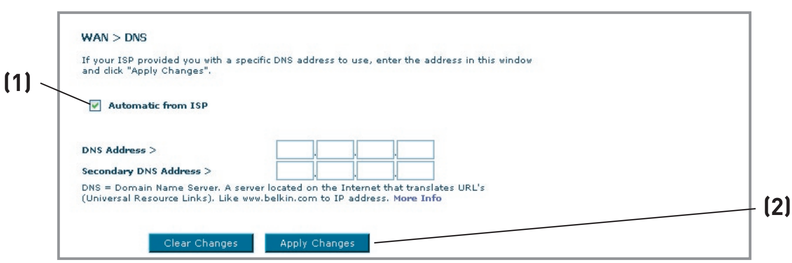
In this mode, the Router simply acts as a bridge passing packets across the DSL port. It requires additional software to be installed on your computers in order to access the Internet.



1. VPI/VCI - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).

DNS (Domain Name Server) Settings

A "Domain Name Server" is a server located on the Internet that translates Universal Resource Links (URLs) like "www.belkin.com" to IP addresses. Many ISPs do not require you to enter this information into the Router. The "Automatic from ISP" box **(1)** should be checked if your ISP did not give you a specific DNS address. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is dynamic or PPPoE, it is likely that you do not have to enter a DNS address. Leave the "Automatic from ISP" box checked. To enter the DNS address settings, uncheck the "Automatic from ISP" box and enter your DNS entries in the spaces provided. Click "Apply Changes" **(2)** to save the settings.



Using Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static host name in any of the many domains DynDNS.org offers, allowing your network computers to be more easily accessed from various locations on the Internet. DynDNS.org provides this service, for up to five host names, free to the Internet community.

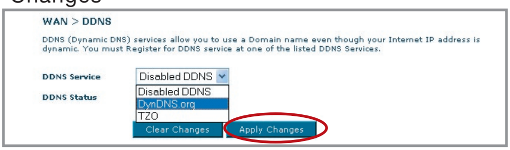
The Dynamic DNSSM service is ideal for a home website, file server, or to make it easy to access your home PC and stored files while you're at work. Using the service can ensure that your host name always points to your IP address, no matter how often your ISP changes it. When your IP address changes, your friends and associates can always locate you by visiting yourname.dyndns.org instead!

To register free for your Dynamic DNS host name, please visit http://www.dyndns.org.

Setting up the Router's Dynamic DNS Update Client

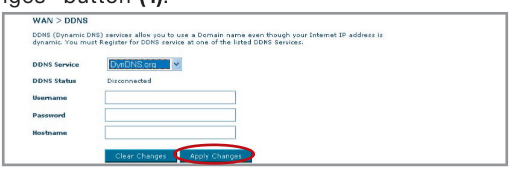
You must register with DynDNS.org's free update service before using this feature. Once you have your registration, follow the directions below.

1. Select "DynDNS.org" from the dropdown box. Click "Apply Changes"



2. Enter your DynDNS.org user name in the "User Name" field **(1)**.
3. Enter your DynDNS.org password in the "Password" field **(2)**.
4. Enter the DynDNS.org domain name you set up with DynDNS.org in the "Domain Name" field **(3)**.
5. Click "Apply Changes" to update your IP address.

Whenever your IP address assigned by your ISP changes, the Router will automatically update DynDNS.org's servers with your new IP address. You can also do this manually by clicking the "Apply Changes" button **(4)**.

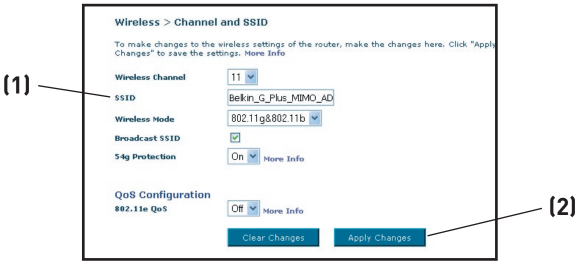


section
1
2
3
4
5
6
7
8
9
10

Wireless

The “Wireless” tab lets you make changes to the wireless network settings. From this tab, you can make changes to the wireless network name (SSID), operating channel, and encryption security settings.

Channel and SSID



1. Changing the Wireless Channel

There are a number of operating channels you can choose from. In the United States, there are 11 channels. In the United Kingdom and most of Europe, there are 13 channels. In a small number of other countries, there are other channel requirements. Your Router is configured to operate on the proper channels for the country you reside in. The default channel is 11 (unless you are in a country that does not allow channel 11). The channel can be changed if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks. For best performance, use a channel that is at least five channels away from the other wireless networks. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. To change the channel, select the channel from the drop-down list. Click “Apply Changes”. The change is immediate.

2. Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. The default SSID of the Router is “belkin54g”. You can change this to anything you want to or you can leave it unchanged. If there are other wireless networks operating in your area, you will want to make sure that your SSID is unique (does not match that of another wireless network in the area). To change the SSID, type in the SSID that you want to use in the SSID field **(1)** and click “Apply Changes” **(2)**. The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.

3. Using the ESSID Broadcast Feature

For security purposes, you can choose not to broadcast your network's SSID. Doing so will keep your network name hidden from computers that are scanning for the presence of wireless networks. To turn off the broadcast of the SSID, remove the tick from the tick box next to the option, Broadcast SSID. The change is immediate. Each computer now needs to be set to connect to your specific SSID; an SSID of "ANY" will no longer be accepted. Refer to the documentation of your wireless network adapter for information on making this change.

Note: This advanced feature should be employed by advanced users only.

4. Using the Wireless Mode Switch

Your router can operate in either two different wireless modes:

- **802.11b & 802.11g-** Choose this option if you plan to have wireless clients of both 802.11b and 802.11g connect to your network.
- **802.11g -** Use this mode if there are no 802.11b clients in the network. This option gives the best performance but will not allow 802.11b clients to connect.

5. Protected Mode Switch

As part of the 802.11g specification, Protected mode ensures proper operation of 802.11g clients and access points when there is heavy 802.11b traffic in the operating environment. When Protected mode is ON, 802.11g scans for other wireless network traffic before it transmits data. Therefore, using this mode in environments with HEAVY 802.11b traffic or interference achieves best performance results. If you are in an environment with very little—or no—wireless network traffic, your best performance will be achieved with Protected mode OFF.

1
2
3
4
5
6
7
8
9
10
section

Encryption/Security

Securing your Wi-Fi Network

Here are a few different ways you can maximize the security of your wireless network and protect your data from prying eyes and ears. This section is intended for the home, home office, and small office user. At the time of this User Manual's publication, there are four encryption methods available.

Name	64-Bit Wired Equivalent Privacy	128-Bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronym	64-bit WEP	128-bit WEP	WPA-TKIP/AES (or just WPA)	WPA2-AES (or just WPA2)
Security	Good	Better	Best	Best
Features	Static keys	Static keys	Dynamic key encryption and mutual authentication	Dynamic key encryption and mutual authentication
	Encryption keys based on RC4 algorithm (typically 40-bit keys)	More secure than 64-bit WEP using a key length of 104 bits plus 24 additional bits of system-generated data	TKIP (Temporal Key Integrity Protocol) added so that keys are rotated and encryption is strengthened	AES (Advanced Encryption Standard) does not cause any throughput loss

WEP (Wired Equivalent Privacy)

WEP is a common protocol that adds security to all Wi-Fi-compliant wireless products. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.

64-Bit WEP

64-bit WEP was first introduced with 64-bit encryption, which includes a key length of 40 bits plus 24 additional bits of system-generated data (64 bits total). Some hardware manufacturers refer to 64-bit as 40-bit encryption. Shortly after the technology was introduced, researchers found that 64-bit encryption was too easy to decode.

128-Bit WEP

As a result of 64-bit WEP's potential security weaknesses, 128Bit WEP was developed as a more secure method of encryption. 128-bit encryption includes a key length of 104 bits plus 24 additional bits of system-generated data (128 bits total). Some hardware manufacturers refer to 128-bit as 104-bit encryption.

Most of the new wireless equipment in the market today supports both 64-bit and 128-bit WEP encryption, but you might have older equipment that only supports 64-bit WEP. All Belkin wireless products will support both 64-bit and 128-bit WEP.

Encryption Keys

After selecting either the "64-bit" or "128-bit WEP" encryption mode, it is critical that you generate an encryption key. If the encryption key is not consistent throughout the entire wireless network, your wireless networking devices will be unable to communicate with one another on your network and you will not be able to successfully communicate within your network.

You can enter your key by typing in the hex key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a key. A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex characters. For 128-bit WEP, you need to enter 26 hex characters.

The WEP passphrase is NOT the same as a WEP key. Your wireless card uses this passphrase to generate your WEP keys, but different hardware manufacturers might have different methods for generating the keys. If you have equipment from multiple vendors in your network, you can use the hex WEP key from your Router or access point and enter it manually into the hex WEP key table in your wireless card's configuration screen.

Using a Hexadecimal Key

A hexadecimal key is a mixture of numbers and letters from A–F and 0–9. 64-bit keys are five two-digit numbers. 128-bit keys are 13 two-digit Characters.

For instance:
AF 0F 4B C3 D4 = 64-bit key
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit key
In the boxes below, make up your key by writing in two characters

between A–F and 0–9 in each box. You will use this key to program the encryption settings on your Router and your wireless computers.

Note to Mac users: Original Apple AirPort® products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) is a new Wi-Fi standard that was designed to improve upon the security features of WEP. To use WPA security, the drivers and software of your wireless equipment must be upgraded to support WPA. These updates will be found on the wireless vendors' websites. There are two types of WPA security: WPA-Personal (PSK) and WPA-Enterprise (RADIUS).

WPA-Personal (PSK)

This method uses what is known as a Pre-Shared key as the Network key. A Network key is basically a password that is between eight and 63 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same Network key to access the network. Typically, this is the mode that will be used in a home environment.

WPA-Enterprise (RADIUS)

With this system, a radius server distributes the Network key to the clients automatically. This is typically found in a business environment. For a list of Belkin wireless products that support WPA, please visit our website at **www.belkin.com/networking**.

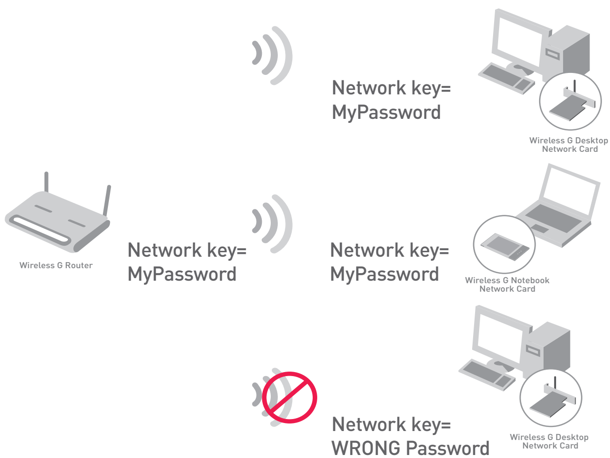
WPA2 (WiFi Protected Access)

WPA2 is the second generation of WPA based 802.11i standard. It offers higher level of wireless security by combining advanced network authentication and stronger AES encryption method. Like WPA security, WPA2 is available in both WPA2-Personal (PSK) mode and WPA2-Enterprise (RADIUS) mode. Typically, WPA2-Personal (PSK) is the mode that will be used in a home environment, while WPA-Enterprise (RADIUS) is implemented in a business environment where an external radius server distributes the network key to the clients automatically.

Sharing the Same Network Keys

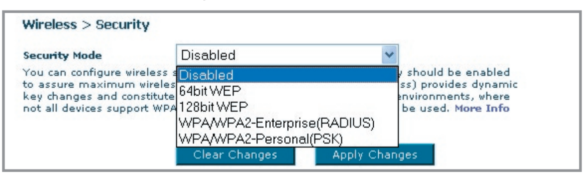
Most Wi-Fi products ship with security turned off. So once you have your network working, you need to activate WEP or WPA or WPA2 and make sure your wireless networking devices are sharing the same Network key.

The Wireless G+ MIMO Desktop Network Card cannot access the network because it is using a different Network key than the Network key that is configured on the Wireless G+ MIMO Router.



Changing the Wireless Security Settings

Your Router is equipped with WPA/WPA2 (Wi-Fi Protected Access), the latest wireless security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). By default, wireless security is disabled. To enable security, you must first determine which standard you want to use. To access the security settings, click **"Security" on the Wireless tab.**



WEP Setup

64-Bit WEP Encryption

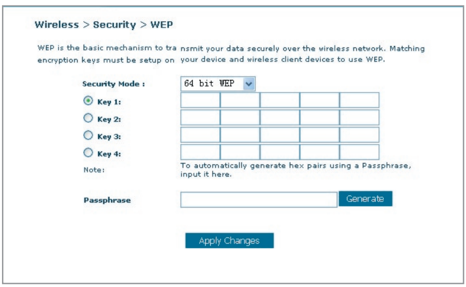
1. Select “64-bit WEP” from the drop-down menu.

2. After selecting your WEP encryption mode, you can enter your key by typing in the hex key manually.

A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex characters.

For instance:

AF 0F 4B C3 D4 = 64-bit WEP key



3. Click “Apply Changes” to finish. Encryption in the Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router or access point from a computer with a wireless client, you will lose your connection until you enable security on your wireless client. Please be sure to write down your key before applying changes

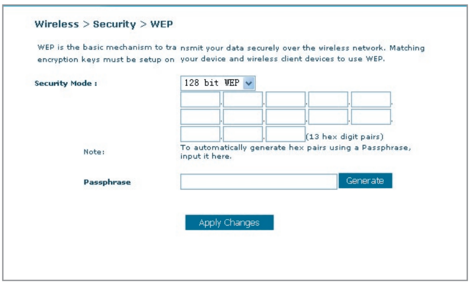
128-Bit WEP Encryption

1. Select "128-bit WEP" from the drop-down menu.
2. After selecting your WEP encryption mode, you can enter your key by typing in the hex key manually.

   A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 hex characters.

   For instance:

   C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key



3. Click "Apply Changes" to finish. Encryption in the Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router or access point from a computer with a wireless client, you will lose your connection until you enable security on your wireless client. Please be sure to write down your key before applying changes.

WPA Setup

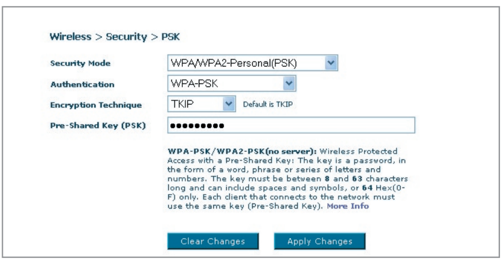
Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this User Manual's publication, a security patch download is available free from Microsoft. This patch works only with the Windows XP operating system. You also need to download the latest driver for your Belkin Wireless G Desktop or Notebook Network Card from the Belkin support site. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as Belkin 802.11g products.

There are two types of WPA security: WPA-Personal (PSK) and WPA-Enterprise (RADIUS). WPA-Personal (PSK) uses a so-called Pre-Shared key as the security key. A Pre-Shared key is a password that is between eight and 63 characters long. It can be a combination of letters, numbers, and other characters. Each client uses the same key to access the network. Typically, this mode will be used in a home environment.

WPA-Enterprise (RADIUS) is a configuration wherein a radius server distributes the keys to the clients automatically. This is typically used in a business environment.

Setting WPA-Personal (PSK)

1. From the "Security Mode" drop-down menu, select "WPA/WPA2-PSK.
2. Select "WPA-PSK" for Authentication.
3. For Encryption Technique, select "TKIP". This setting will have to be identical on the clients that you set up.
4. Enter your Pre-Shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".



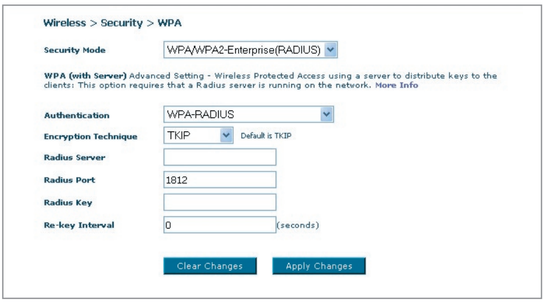
5. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Setting WPA-Enterprise (RADIUS) Settings

If your network uses a radius server to distribute keys to the clients, use this setting.

1. From the "Security Mode" drop-down menu, select "WPA/WPA2—Enterprise (RADIUS)

2. Select “WPA-RADIUS” for Authentication
3. For Encryption Technique, select “TKIP”. This setting will have to be identical on the clients that you set up
4. Enter the IP address of the radius server into the “Radius Server” fields.
5. Enter the radius key into the “Radius Key” field.
6. Enter the key interval. Key interval is how often the keys are distributed (in packets).
7. Click “Apply Changes” to finish. You must now set all clients to match these settings.



WPA2 Requirements

IMPORTANT: In order to use WPA2 security, all your computers and wireless client adapters must be upgraded with patches, driver, and client utility software that supported WPA2. At the time of this User Manual’s publication, a couple security patches are available, for free download, from Microsoft. These patches work only with the Windows XP operating system. Other operating systems are not supported at this time.

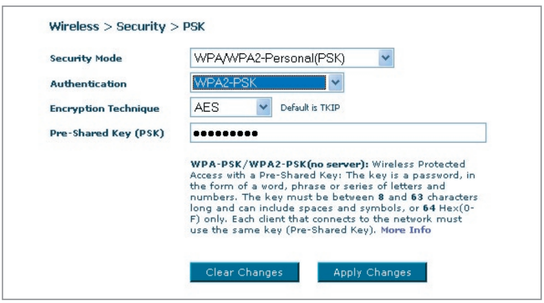
For Windows XP computer that does not have Service Pack 2 (SP2), a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access (KB 826942)” is available for free download at http://support.microsoft.com/?kbid=826942

For Windows XP with Service Pack 2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB893357). The update can be download from: http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

IMPORTANT: You also need to ensure that all your wireless client cards / adapters support WPA2, and that you have downloaded and installed the latest driver. Most of the Belkin Wireless cards have update driver available for download from the Belkin support site: www.belkin.com/networking.

Setting WPA2-Personal (PSK)

1. From the "Security Mode" drop-down menu, select "WPA/WPA2-PSK (PSK)".
2. Select "WPA2-Personal (PSK)" for Authentication.
3. For Encryption Technique, select "AES" . This setting will have to be identical on the clients that you set up.
4. Enter your Pre-Shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".



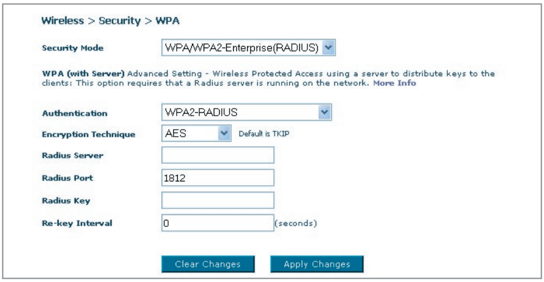
5. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Setting WPA2-Enterprise (RADIUS) Settings

If your network uses a radius server to distribute keys to the clients, use this setting.

1. From the "Security Mode" drop-down menu, select "WPA/WPA2—Enterprise (RADIUS)".
2. Select "WPA2-RADIUS" for Authentication
3. For Encryption Technique, select "AES". This setting will have to be identical on the clients that you set up

4. Enter the IP address of the radius server into the “Radius Server” fields.
5. Enter the radius key into the “Radius Key” field.
6. Enter the key interval. Key interval is how often the keys are distributed (in packets).
7. Click “Apply Changes” to finish. You must now set all clients to match these settings.



IMPORTANT: Make sure your wireless computers are updated to work with WPA2 and have the correct settings to get proper connection to the Router.

Configuring your Computer’s Network Adapter to Use Security

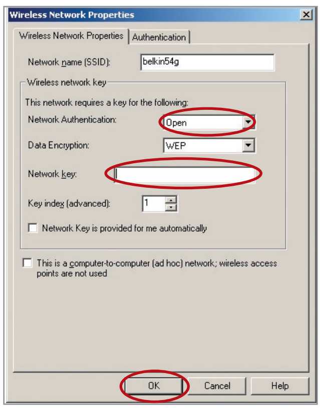
Note: This section provides information on how to configure network adapter in your computers to use security. At this point, you should already have your Wireless Router or access point set to use WPA2 or WPA or WEP. In order for you to gain a wireless connection, you will need to set your wireless notebook card and wireless desktop card to use the same security settings.

Belkin G+ MIMO Network Cards feature easy-to-use Wireless Networking Utility. Simply click on your wireless network name (SSID) from the Available Networks list and enter your Pre-Share Key (PSK). For more information please refer to Belkin Network Card’s user manual.

Most computers can also setup to work with the Router from Wireless Network Properties screen build-in your Microsoft Windows operating system. The following are two of the examples:

Connecting your Computer to a Wireless Network that Requires a 64-Bit or 128-Bit WEP Key

1. Double-click the "Signal Indicator" icon to bring up the "Wireless Network" screen. The "Advanced" button will allow you to view and configure more options of your wireless card.
2. Under the "Wireless Network Properties" tab, select a network name from the "Available networks" list and click "Configure".
3. Under "Data Encryption" select "WEP".
4. Ensure the check box "Network key is provided for me automatically" at the bottom is unchecked. If you are using this computer to connect to a corporate network, please consult your network administrator if this box needs to be checked.
5. Type your WEP key in the "Network key" box.

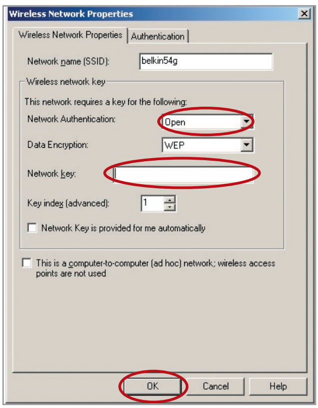


Important: A WEP key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 characters. For 64-bit WEP, you need to enter 10 characters. This Network key needs to match the key you assign to your Wireless Router or access point.

6. Click "OK" to save the settings.

Connecting your Computer to a Wireless Network that Requires WPA-PSK (no server)

1. Double-click the "Signal Indicator" icon to bring up the "Wireless Network" screen. The "Advanced" button will allow you to view and configure more options of your wireless card.
2. Under the "Wireless Networks" tab, select a network name from the "Available networks" list and click "Configure".
3. Under "Network Authentication" select "WPA-PSK (No Server)".
4. Type your WPA key in the "Network key" box.

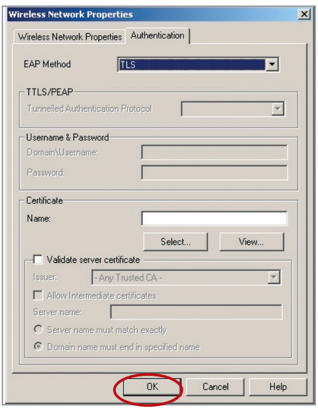


Important: WPA-PSK is a mixture of numbers and letters from A–Z and 0–9. For WPA-PSK you can enter eight to 63 characters. This Network key needs to match the key you assign to your Wireless Router or access point.

5. Click "OK" to save the settings.

Connecting your Computer to a Wireless Network that Requires WPA (with radius server)

1. Double-click the "Signal Indicator" icon to bring up the "Wireless Network" screen. The "Advanced" button will allow you to view and configure more options of your wireless card.
2. Under the "Wireless Networks" tab, select a network name from the "Available networks" list and click "Configure".
3. Under "Network Authentication" select WPA.
4. Under the "Authentication" tab, select the settings that are indicated by your network administrator.



5. Click "OK" to save the settings.

Setting Up WPA/WPA2 for a Non-Belkin Wireless Desktop and Wireless Notebook Cards

For non-Belkin WPA Wireless Desktop and Wireless Notebook Cards that are not equipped with WPA/WPA2-enabled software, a file from Microsoft called "Windows XP Support Patch for Wireless Protected Access" is available as a free download.

Please Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time.

Important: You also need to ensure that the wireless card manufacturer supports WPA/WPA2 and that you have downloaded and installed the latest driver from their support site.

Supported Operating Systems:

- **Windows XP Professional**
- **Windows XP Home Edition**

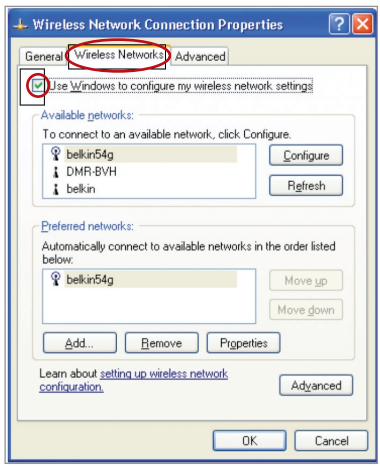
Setting Up Windows XP Wireless Network Utility to Use WPA/WPA2-PSK

In order to use WPA-PSK, ensure you are using Windows Wireless Network Utility by doing the following:

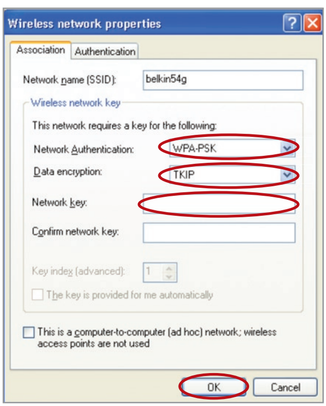
1. Under Windows XP, click "Start > Control Panel > Network Connections".

2. Right-click on "Wireless Network Connection", and select "Properties".

3. Clicking on the "Wireless Networks" tab will display the following screen. Ensure the "Use Windows to configure my wireless network settings" check box is checked.



4. Under the "Wireless Networks" tab, click the "Configure" button, and you will see the following screen.



5. For a home or small business user, select "WPA-PSK" or WPA2-PSK under "Network Authentication".

Note: Select "WPA" if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server. Please consult your network administrator for further information.

6. Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the Router that you set up.

7. Type in your encryption key in the “Network Key” box.

Important: Enter your Pre-Shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.

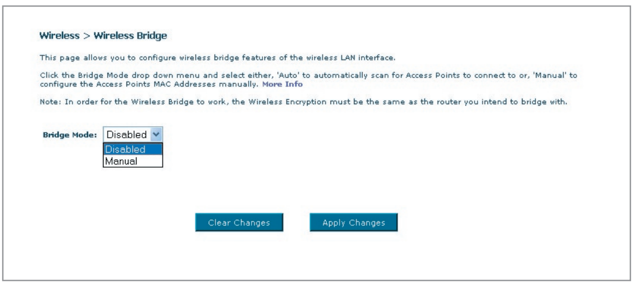
8. Click “OK” to apply settings.

Wireless Bridge

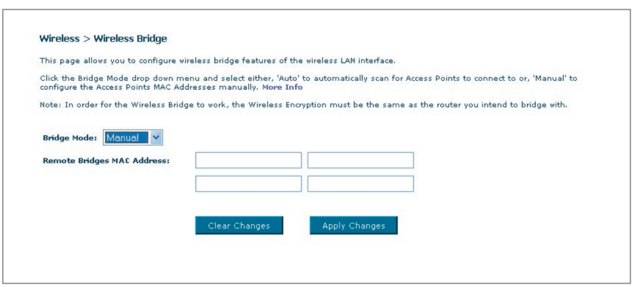
Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

Click on the Drop down menu next to ‘Bridge Mode’ to select either:

Disabled:
To disable Wireless Bridging (default)



Manual:
To enter the wireless MAC address(es) of the Access Points to bridge with, manually.



1 Wireless channels must match between Router and AP.

2 Security settings (WEP) must match between Router and AP.

3 If MAC filtering is enabled, user must be sure to add the WLAN MAC address(es) of the Router/AP in order to allow communication with each other.

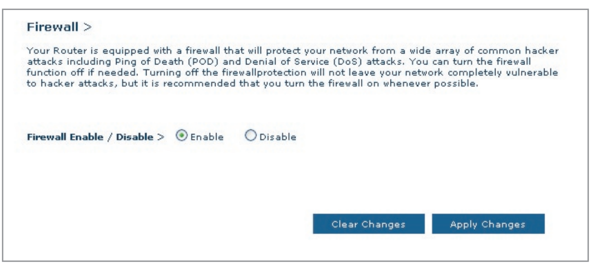
4 If using a network protected by WPA, the SSID on both Access Points must be the same.

Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:

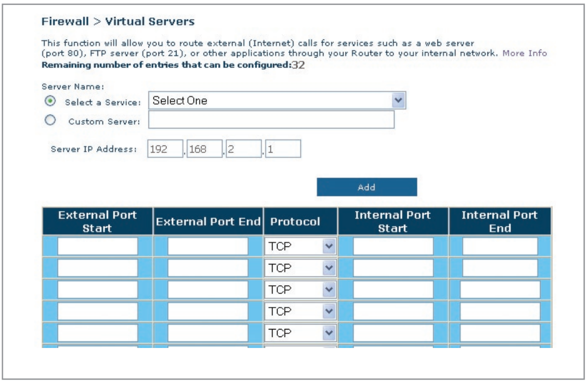
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be “Stealth”, meaning that essentially they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.



Virtual Servers

Virtual servers allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications, through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be "seen". If you need to configure the virtual server function for a specific application, you will need to contact the application vendor to find out which port settings you need. You can manually input this port information into the Router.



Choosing an Application

A list of popular applications has been included to choose from. Click on "Select a Service" then select your application from the drop-down list. The settings will be transferred to the first row available. Click "Add" to save the setting for that application.

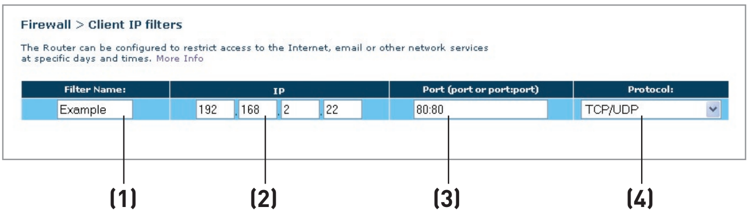
Manually Entering Settings into the Virtual Server

To manually enter settings, click on "Custom Server" and enter a name for the server. Enter the Server IP address in the space provided for the internal machine and the port(s) required to pass. Then select the protocol type (TCP or UDP), and then click "Add".

Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Client IP Filters

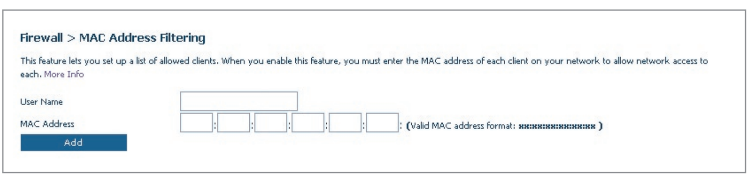
The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times.



To restrict Internet access to a single computer for example, enter a name of the filter in "Filter Name" box **(1)** and IP address of the computer you wish to restrict access to in the IP field **(2)**. Next, enter "80:80" in the Port field **(3)**. Select protocol from the "Protocol" drop-down box **(4)**. Click "Apply Changes". The computer at the IP address you specified will now be blocked from Internet access.

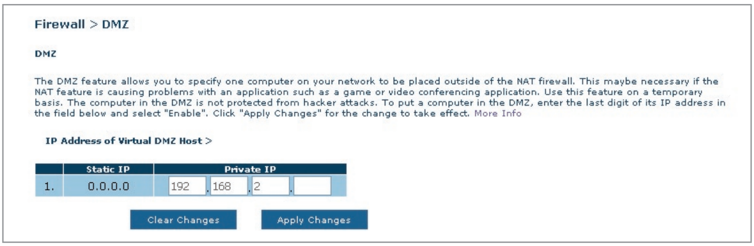
MAC Address Filtering

The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter a name for the user and the MAC address of each client on your network to allow network access. Next, click "Add" to save the settings.



DMZ (Demilitarized Zone)

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.**

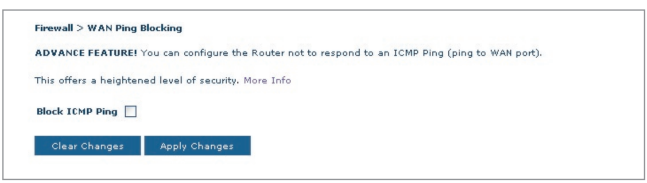


To put a computer in the DMZ, enter its LAN IP address in the "Private IP" field and click "Apply Changes" for the change to take effect.

Blocking an ICMP Ping

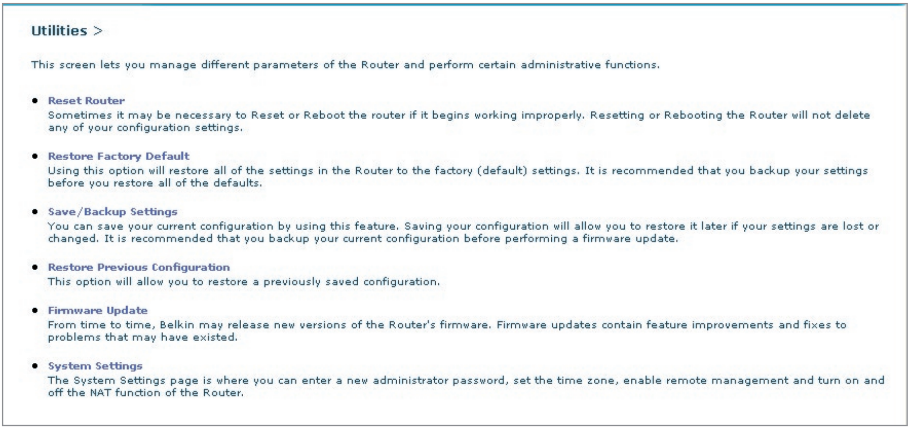
Computer hackers use what is known as "pinging" to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an ICMP ping from the outside. This heightens the level of security of your Router.

To turn off the ping response, select "Block ICMP Ping" **(1)** and click "Apply Changes". The Router will not respong to an ICMP Ping.



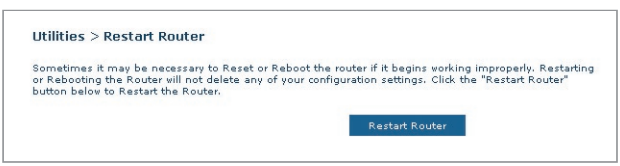
Utilities

The “Utilities” screen lets you manage different parameters of the Router and perform certain administrative functions.



Restart Router

Sometimes it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.



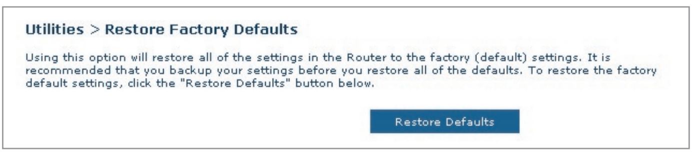
Restarting the Router to Restore Normal Operation

1. Click the “Restart Router” button.
2. The following message will appear. Click “OK” to restart your Router.

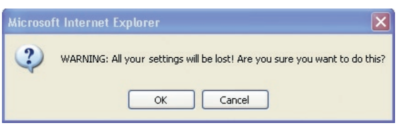


Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.

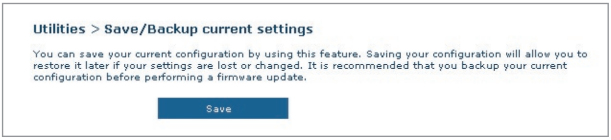


1. Click the “Restore Defaults” button.
2. The following message will appear. Click “OK” to restore factory defaults.

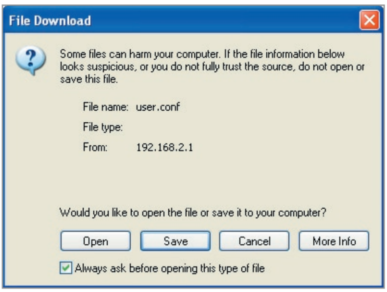


Saving/Backup Current Settings

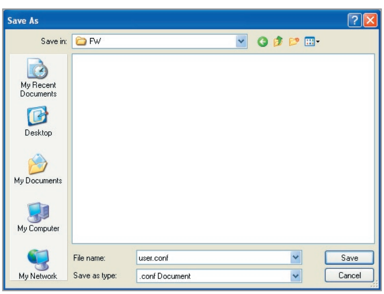
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.



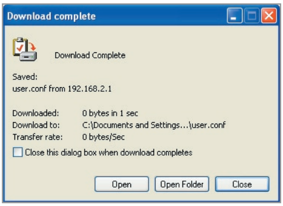
1. Click “Save”. A window called “File Download” will open. Click “Save”.



2. A window will open that allows you to select the location in which to save the configuration file. Select a location. There are no restrictions on the file name, however, be sure to name the file so you can locate it yourself later. When you have selected the location and entered the file name, click “Save”.



3. When the save is complete, you will see the window below. Click “Close”.

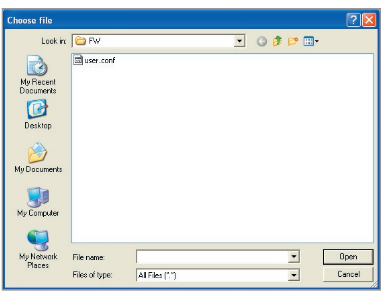


The configuration is now saved.

Restore Previous Settings

This option will allow you to restore a previously saved configuration.

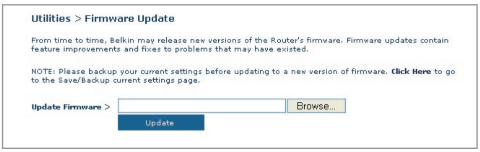
1. Click “Browse”. A window will open that allows you to select the location of the configuration file. All configuration files end with a “.conf”. Locate the configuration file you want to restore and double-click on it.



2. Then, click “Open”.

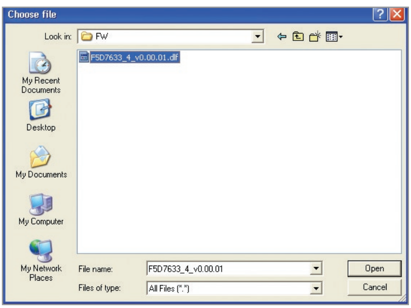
Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed. When Belkin releases new firmware, you can download the firmware from the Belkin update website and update your Router's firmware to the latest version.



Updating the Router's Firmware

1. In the "Firmware Update" page, click "Browse". A window will open that allows you to select the location of the firmware update file.



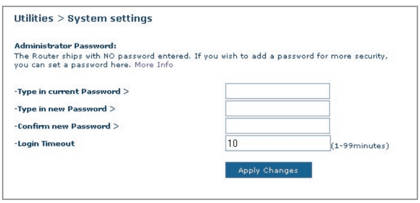
2. Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.
3. Click "Update" to upgrade to the latest firmware version.

System Settings

The "System Settings" page is where you can enter a new administrator password, set the time zone, enable remote management, and turn on and off the UPnP function of the Router.

Setting or Changing the Administrator Password

The Router ships with NO password entered. If you wish to add a password for greater security, you can set a password here. Write down your password and keep it in a safe place, as you will need it if you need to log into the Router in the future. It is also recommended that you set a password if you plan to use the remote management feature of your Router.



Changing the Login Time-Out Setting

The login time-out option allows you to set the period of time that you can be logged into the Router's advanced setup interface. The timer starts when there has been no activity. For example, you have made some changes in the advanced setup interface, then left your computer alone without clicking "Logout". Assuming the time-out is set to 10 minutes, then 10 minutes after you leave, the login session will expire. You will have to log into the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes.

Note: Only one computer can be logged into the Router's advanced setup interface at one time.

Setting the Time and Time Zone

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering.

Select desired NTP time servers and the time zone that you reside in, then click "Apply Changes". The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.



Enabling Remote Management

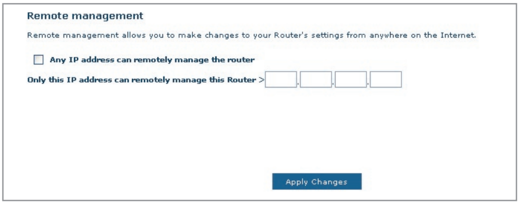
Before you enable this advanced feature of your Belkin Router, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD**. Remote management allows you to make changes to your Router's settings from anywhere on the Internet.

Click on the "Change Settings" button to bring up the "Remote Management" page.

There are two methods of remotely managing the Router. The first is to allow access to the Router from anywhere on the Internet by selecting "Any IP address can remotely manage the Router". By typing in your WAN IP address from any computer on the Internet, you will be presented with a login screen where you need to type in the password of your Router.

The second method is to allow a specific IP address only to remotely manage the Router. This is more secure, but less convenient. To use this method, enter the IP address you know you will be accessing the Router from in the space provided and select "Only this IP address can remotely manage the Router". Before you enable this function, it is STRONGLY RECOMMENDED that you set your administrator password. Leaving the password empty will potentially open your Router to intrusion.

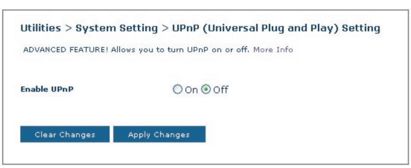
Click on the “Apply Changes” button to save your settings.



Enabling/Disabling UPnP

UPnP (Universal Plug-and-Play) is yet another advanced feature offered by your Belkin Router. It is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router’s firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports, and in some instances, setting trigger ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically “telling” the Router which way it needs the firewall configured. The Router ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish to take advantage of the UPnP features, you can enable the UPnP feature.

Click on the “Change Setting” button to bring up the “UPnP Setting” page. Then select “On” for “Enable UPnP”. Click on the “Apply Changes” button to save your settings.



1
2
3
4
5
6
7
8
9
10
section

Problem:

The ADSL LED is not on.

Solution:

1. Check the connection between the Router and ADSL line. Make sure the cable from the ADSL line is connected to the port on the Router labeled “DSL Line”.
2. Make sure the Router has power. The Power LED ⏻ on the front panel should be illuminated.

Problem:

The Internet LED is not on.

Solution:

1. Make sure the cable from the ADSL line is connected to the port on the Router labeled “DSL Line” and the ADSL LED ☎ is on.
2. Make sure you have the correct VPI/VCI, user name, and password from your ISP provider.

Problem:

My connection type is static IP address. I can’t connect to the Internet.

Solution:

Since your connection type is static IP address, your ISP must assign you the IP address, subnet mask, and gateway address. Instead of using the Wizard, go to “Connection Type”, and then select your connection type. Click “Next”, select “Static IP”, and enter your IP address, subnet mask, and default gateway information.

Problem:

I’ve forgotten or lost my password.

Solution:

Press and hold the “Reset” button on the rear panel for at least 10 seconds to restore the factory defaults.

Problem:

My wireless PC cannot connect to the Router.

Solution:

1. Make sure the wireless PC has the same SSID settings as the Router, and you have the same security settings on the clients such as WPA or WEP encryption.
2. Make sure the distance between the Router and wireless PC are not too far away.

Problem:

The wireless network is often interrupted.

Solution:

1. Move your wireless PC closer to the Router to find a better signal.
2. There may also be interference, possibly caused by a microwave oven or 2.4GHz cordless phones. Change the location of the Router or use a different wireless channel.

Problem:

I can’t connect to the Internet wirelessly.

Solution:

If you are unable to connect to the Internet from a wireless computer, please check the following items:

1. Look at the lights on your Router. If you are using a Belkin Router, the lights should be as follows:
   - The “Power” light should be on.
   - The “DSL LED”v should be on, and not blinking.
   - The “Internet LED” should be either on or blinking.
2. Open your wireless utility software by clicking on the icon in the system tray at the bottom right-hand corner of the screen. If you’re using a Belkin Wireless Card, the tray icon should look like this.  The icon may be red or green.
3. The exact window that opens will vary depending on the model of wireless card you have; however, any of the utilities should have a list of “Available Networks”— those wireless networks it can connect to.

Does the name of your wireless network appear in the results?

Yes, my network name is listed—go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, but my network name is listed".

No, my network name is not listed—go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, and my network name is not listed".

Problem:

I can't connect to the Internet wirelessly, but my network name is listed.

Solution:

If the name of your network is listed in the "Available Networks" list, please follow the steps below to connect wirelessly:

1. Click on the correct network name in the "Available Networks" list.
2. If the network has security (encryption) enabled, you will need to enter the network key. For more information regarding security, see the page entitled: "Changing the Wireless Security Settings".
3. Within a few seconds, the tray icon in the lower left-hand corner of your screen should turn green, indication a successful connection to the network.



Problem:

I can't connect to the Internet wirelessly, and my network name is not listed.

Solution

If the correct network name is not listed under "Available Networks" in the wireless utility, please attempt the following troubleshooting steps:

1. Temporarily move computer, if possible, five to 10 feet from the Router. Close the wireless utility, and re-open it. If the

correct network name now appears under "Available Networks", you may have a range or interference problem. Please see the suggestions discussed in Appendix B entitled "Important Factors for Placement and Setup".

2. Using a computer that is connected to the Router via a network cable (as opposed to wirelessly), ensure that "Broadcast SSID" is enabled. This setting is found on the Router's wireless "Channel and SSID" configuration page.

   If you are still unable to access the Internet after completing these steps, please contact Belkin Technical Support.

Problem:

My wireless network performance is inconsistent.

Data transfer is sometimes slow.

Signal strength is poor.

Difficulty establishing and/or maintaining a Virtual Private Network (VPN) connection.

Solution:

Wireless technology is radio-based, which means connectivity and the throughput performance between devices decreases when the distance between devices increases. Other factors that will cause signal degradation (metal is generally the worst culprit) are obstructions such as walls and metal appliances. As a result, the typical indoor range of your wireless devices will be between 100 to 200 feet. Note also that connection speed may decrease as you move farther from the Router or access point.

In order to determine if wireless issues are related to range, we suggest temporarily moving the computer, if possible, five to 10 feet from the Router.

Changing the wireless channel - Depending on local wireless traffic and interference, switching the wireless channel of your network can improve performance and reliability. The default channel the Router is shipped with is channel 11, you may choose from several other channels depending on your region; see the section entitled "Changing the Wireless Channel" on page 37 for instructions on how to choose other channels.

Limiting the wireless transmit rate - Limiting the wireless transmit rate can help improve the maximum wireless range, and connection stability. Most wireless cards have the ability to limit the transmission rate. To change this property, go to the Windows Control Panel, open “Network Connections” and double-click on your wireless card’s connection. In the “Properties” dialog, select the “Configure” button on the “General” tab (Windows 98 users will have to select the wireless card in the list box and then click “Properties”), then choose the “Advanced” tab and select the rate property. Wireless client cards are usually set to automatically adjust the wireless transmit rate for you, but doing so can cause periodic disconnects when the wireless signal is too weak; as a rule, slower transmission rates are more stable. Experiment with different connection rates until you find the best one for your environment; note that all available transmission rates should be acceptable for browsing the Internet. For more assistance, see your wireless card’s user manual.

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Belkin Router or Belkin Access Point.

Solution

1. Log into your Wireless Router or access point.
2. Open your web browser and type in IP address of the Wireless Router or access point. (The Router default is 192.168.2.1, the 802.11g access point is 192.168.2.254). Log into your Router by clicking on the “Login” button in the top right-hand corner of the screen. You will be asked to enter your password. If you never set a password, leave the password field blank and click “Submit”.
3. Click the “Wireless” tab on the left of your screen. Select the “Encryption” or “Security” tab to get to the security settings page.
4. Select “128-bit WEP” from the drop-down menu.
5. After selecting your WEP encryption mode, you can type in your hex WEP key manually, or you can type in a passphrase in the “Passphrase” field and click “Generate” to create a WEP key from the passphrase. Click “Apply Changes” to finish. You must now set all of your clients to match these settings. A hex (hexadecimal) key is a mixture of numbers and letters from A-F

1 2 3 4 5 6 7 8 9 10 section

and 0-9. For 128-bit WEP, you need to enter 26 hex characters.

For example:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key

6. Click "Apply Changes" to finish. Encryption in the Wireless Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router or Access Point from a computer with a wireless client, you will need to ensure that security is turned on for this wireless client. If this is not done, you will lose your wireless connection.

Note to Mac users: Original Apple AirPort® products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your Apple AirPort product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Belkin Wireless Card.

Solution:

The Wireless Card must use the same key as the Wireless Router or access point. For instance, if your Wireless Router or access point uses the key 00112233445566778899AABBCC, then the Wireless Card must be set to the exact same key.

1. Double-click the "Signal Indicator" icon to bring up the Wireless "Network" screen.
2. The "Advanced" button will allow you to view and configure more options of the Card.
3. Once the "Advanced" button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the "Wireless Network Properties" tab, select a network name from the "Available networks" list and click the "Properties" button.
5. Under "Data Encryption" select "WEP".

6. Ensure the check box "The key is provided for me automatically" at the bottom is unchecked. If you are using this computer to connect to a corporate network, please consult your network administrator if this box needs to be checked.
7. Type your WEP key in the "Network key" box.

   Important: A WEP key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 keys. This Network key needs to match the key you assign to your Wireless Router or access point.

   For example:
   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key
8. Click "OK", and then "Apply" to save the settings.

If you are **NOT** using a Belkin Wireless Card, please consult the manufacturer for that wireless client card's user manual.

Problem:

Do Belkin products support WPA?

Solution

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this FAQ publication, a security patch download is available, for free, from Microsoft. This patch works only with the Windows XP operating system.

Download the patch here:

http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

You also need to download the latest driver for your Belkin Wireless 802.11g Desktop or Notebook Network Card from the Belkin support site. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as Belkin 802.11g products.

Download the latest driver at:
http://web.belkin.com/support/networkingsupport.asp.

WPA support will also be automatically installed if you upgrade your system to Windows XP Service pack 2. Detials about this can be found at http://support.microsoft.com

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Router or Belkin Access Point for a home network.

Solution:

1. From the "Security Mode" drop-down menu, select "WPA-PSK (no server)".
2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols or spaces. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".
4. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Router or Belkin Access Point for a business.

Solution:

If your network uses a radius server to distribute keys to the clients, use this setting. This is typically used in a business environment.

1. From the "Security Mode" drop-down menu, select "WPA (with server)".
2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.
3. Enter the IP address of the radius server into the "Radius Server" fields.
4. Enter the radius key into the "Radius Key" field.
5. Enter the key interval. Key interval is how often the keys are distributed (in packets).
6. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Card for a home network.

Solution:

Clients must use the same key that the wireless router or access point uses. For instance if the key is “Smith Family Network Key” in the wireless router or access point, the clients must also use that same key.

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the Card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Network Authentication” select “WPA-PSK (no server)”.
6. Type your WPA key in the “Network key” box.

   Important: WPA-PSK is a mixture of numbers and letters from A–Z and 0–9. For WPA-PSK you can enter eight to 63 characters. This network key needs to match the key you assign to your Wireless Router or access point.
7. Click “OK, then “Apply” to save the settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Card for a business.

Solution:

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the Card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the

advanced features of the Belkin Wireless Card.

4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Network Authentication” select “WPA”.
6. In the “Authentication” tab, select the settings that are indicated by your network administrator.
7. Click “OK, then “Apply” to save the settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security and I am **NOT** using a Belkin Wireless Card for a home network.

Solution:

If you are **NOT** using a Belkin Wireless Desktop or Wireless Notebook Network Card and it is not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available for free download. Download the patch from Microsoft by searching the knowledge base for Windows XP WPA.

Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time. You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.

Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

Enabling WPA-PSK (no server)

1. Under Windows XP, click “Start > Control Panel > Network Connections”.
2. Right-clicking on the “Wireless Networks” tab will display the following screen. Ensure the “Use Windows to configure my wireless network settings” check box is checked.
3. Under the “Wireless Networks” tab, click the “Configure” button, and you will see the following screen.

4. For a home or small business user, select “WPA-PSK” under “Network Administration”.

   Note: Select WPA (with radius server) if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server. Please consult your network administrator for further information.

5. Select “TKIP” or “AES” under “Date Encryption”. This setting will have to be identical to the wireless router or access point that you set up.

6. Type in your encryption key in the “Network Key” box.

   Important: Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.

7. Click “OK” to apply settings.

What is the difference between 802.11b, 802.11g, G+ MIMO, and Pre-N?

Currently there are four levels of wireless networking standards, which transmit data at very different maximum speeds. Each is based on the designation 802.11(x), so named by the IEEE, the board that is responsible for certifying networking standards. The most common wireless networking standard, 802.11b, transmits information at 11Mbps; 802.11a and 802.11g work at 54Mbps; G+ MIMO works at 54Mbps; and Pre-N works at 108Mbps.

Wireless Comparison Chart

Wireless Technology	802.11b	G (802.11g)	G+ (802.11g with HSM)	G+ MIMO(802.11g with MIMO MRC)	Belkin Pre-N(802.11g with TrueMIMO)
Speed*	11Mbps link rate / Baseline	5x faster than 802.11b*	10x faster than 802.11b*	10x faster than 802.11b*	15x faster than 802.11b*
Frequency	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz
Compatibility	Compatible with 802.11g	Compatible with 802.11b/g	Compatible with 802.11b/g	Compatible with 802.11b/g	Compatible with 802.11g or 802.11b
Coverage*	typically 100–200 ft. indoors	Up to 400ft*	Up to 700ft*	Up to 1000ft*	Up to 1400ft*
Advantage	Mature—legacy technology	Common—widespread use for Internet sharing	Enhanced speed and coverage	Better coverage and consistent speed at range	Leading edge— best coverage and throughput

*Distance and connection speeds will vary depending on your networking environment.

Appendix A: Glossary

IP Address

The “IP address” is the internal IP address of the Router. To access the advanced setup interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type in the new IP address and click “Apply Changes”. The IP address you choose should be a non-routable IP. Examples of a non-routable IP are:

192.168.x.x (where x is anything between 0 and 255)

10.x.x.x (where x is anything between 0 and 255)

Subnet Mask

Some networks are far too large to allow all traffic to flood all its parts. These networks must be broken down into smaller, more manageable sections, called subnets. The subnet mask is the network address plus the information reserved for identifying the “subnetwork”.

DNS

DNS is an acronym for Domain Name Server. A Domain Name Server is a server located on the Internet that translates URLs (Universal Resource Links) like www.belkin.com to IP addresses. Many ISPs do not require you to enter this information into the Router. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is Dynamic or PPPoE, it is likely that you do not have to enter a DNS address.

PPPoE

Most ADSL providers use PPPoE as the connection type. If you use an ADSL modem to connect to the Internet, your ISP may use PPPoE to log you into the service.

Your connection type is PPPoE if:

1. Your ISP gave you a user name and password which is required to connect to the Internet.
2. Your ISP gave you software such as WinPoET or Enternet300 that you use to connect to the Internet.
3. You have to double-click on a desktop icon other than your browser to get on the Internet.

   To set the Router to use PPPoE, type in your user name and password in the spaces provided. After you have typed in your information, click "Apply Changes".

After you apply the changes, the "Internet Status" indicator will read "connection OK" if your Router is set up properly.

PPPoA

Enter the PPPoA information in the provided spaces, and click "Next". Click "Apply" to activate your settings.

1. User name - Enter the user name. (Assigned by your ISP).
2. Password - Enter your password. (Assigned by your ISP).
3. Retype Password - Confirm the password. (Assigned by your ISP).
4. VPI/VCI - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).

Disconnect after X...

This feature is used to automatically disconnect the Router from your ISP when there is no activity for a specified period of time. For instance, placing a check mark next to this option and entering “5” into the minute field will cause the Router to disconnect from the Internet after five minutes of no Internet activity. This option should be used if you pay for your Internet service by the minute.

Channel and SSID

To change the channel of operation of the Router, select the desired channel from the drop-down menu and select your channel. Click “Apply Changes” to save the setting. You can also change the SSID. The SSID is the equivalent to the wireless network’s name. You can make the SSID anything you want to. If there are other wireless networks in your area, you should give your wireless network a unique name. Click inside of the SSID box and type in a new name. Click “Apply Changes” to make the change.

ESSID Broadcast

Many wireless network adapters currently on the market possess a feature known as site survey. It scans the air for any available network and allows each computer to automatically select a network from the survey. This occurs if the computer’s SSID is set to “ANY”. Your Belkin Router can block this random search for a network. If you disable the “ESSID Broadcast” feature, the only way a computer can join your network is by its SSID being set to the specific name of the network (like WLAN). Be sure that you know your SSID (network name) before enabling this feature. It is possible to make your wireless network nearly invisible. By turning off the broadcast of the SSID, your network will not appear in a site survey. Obviously, turning off the broadcast feature of the SSID helps increase security.

Encryption

Setting encryption can help keep your network secure. The Router uses Wired Equivalent Privacy (WEP) and WIFI protested Access (WPA) encrytion to protect to protect your data and features two rates of encryption: 64-bit and 128-bit. Encryption works on a system of keys. The key on the computer must match the key on the Router,

and there are two ways to make a key. The easiest is to let the Router's software convert a passphrase you've created into a key. The advanced method is to enter the keys manually.

Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be "seen". If you need to configure the virtual server function for a specific application, you will need to contact the application vendor to find out which port settings you need.

To manually enter settings, enter the IP address in the space provided for the internal machine, the port type (TCP or UDP), and the LAN and public port(s) required to pass. Then select "Enable" and click "Set". You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Client IP Filters

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

MAC Address Filtering

The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client on your network to allow network access to each or copy the MAC address by selecting the name of the computer from the "DHCP Client List". To enable this feature, select "Enable". Next, click "Apply Changes" to save the settings.

DMZ

If you have a client PC that cannot run an Internet application

properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** To put a computer in the DMZ, enter the last digits of its LAN IP address in the “Static IP” field and click “Apply Changes” for the change to take effect.

If you have only one public (WAN) IP address, then you can leave the public IP to “0.0.0.0”. If you are using multiple public (WAN) IP addresses, it is possible to select which public (WAN) IP address the DMZ host will be directed to. Type in the public (WAN) IP address you wish the DMZ host to direct to, enter the last two digits of the IP address of the DMZ host computer, and click “Apply Changes”.

Administrator Password

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password from your Router's web-based user interface. Keep your password in a safe place as you will need this password if you need to log into the Router in the future. It is **STRONGLY RECOMMENDED** that you set a password if you plan to use the remote management feature. The login time-out option allows you to set the period of time that you can be logged into the Router's advanced setup interface. The timer starts when there has been no activity. For example, you have made some changes in the advanced setup interface, then left your computer alone without clicking "Logout".

Assuming the time-out is set to 10 minutes, then 10 minutes after you leave, the login session will expire. You will have to log into the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes. Note, only one computer can be logged into the Router's advanced setup interface at a time.

Time and Time Zone

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in. If you reside in an area that observes daylight saving time, then place a check mark in the box next to "Enable Daylight Saving". The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response.

Remote Management

Before you enable this function, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD**. Remote management allows you to make changes to your Router's settings from anywhere on the Internet.

UPnP

UPnP (Universal Plug-and-Play) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports and in some instances setting trigger ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish to take advantage of the UPnP features, you can enable the UPnP feature. Simply select "Enable" in the "UPnP Enabling" section of the "Utilities" page. Click "Apply Changes" to save the change.

Appendix B: Important Factors for Placement and Setup

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

1. **Wireless Router (or Access Point) Placement**

   Place your Wireless Router (or access point), the central connection point of your network, as close as possible to the center of your wireless network devices.

   To achieve the best wireless network coverage for your "wireless clients" (i.e., computers enabled by Belkin Wireless Notebook Network Cards, Wireless Desktop Network Cards, and Wireless USB Adapters):

   - Ensure that your Wireless Router's (or access point's) networking antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your Wireless Router (or access point) itself is positioned vertically, point the antennas a much as possible in an upward direction.
   - In multistory homes, place the Wireless Router (or access point) on a floor that is as close to the center of the home as possible. This may mean placing the Wireless Router (or access point) on an upper floor.
   - Try not to place the Wireless Router (or access point) near a cordless 2.4GHz phone.

2. **Avoid Obstacles and Interference**

   Avoid placing your Wireless Router (or access point) near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

   - Refrigerators
   - Washers and/or dryers
   - Metal cabinets
   - Large aquariums
   - Metallic-based UV tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal's path (between your computers and Wireless Router or access point).

3. **Cordless Phones**

If the performance of your wireless network is impaired after attending to the above issues, and you have a cordless phone:

- Try moving cordless phones away from Wireless Routers (or access points) and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Wireless Router (or access point) to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

4. **Choose the "Quietest" Channel for your Wireless Network**

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with yours.

Use the Site Survey capabilities found in the Wireless LAN Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's manual), and move your Wireless Router (or access point) and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices.

For Belkin wireless networking products, use the detailed Site Survey and wireless channel information included in your User Manual.

These guidelines should allow you to cover the maximum possible area with your Wireless Router (or access point). Should you need to cover an even wider area, we suggest the Belkin Wireless Range Extender/Access Point.

5. Secure Connections, VPNs, and AOL

Secure connections typically require a user name and password, and are used where security is important. Secure connections include:

- Virtual Private Network (VPN) connections, often used to connect remotely to an office network
- The "Bring Your Own Access" program from America Online (AOL), which lets you use AOL through broadband provided by another cable or DSL service
- Most online banking websites
- Many commercial websites that require a user name and password to access your account

Secure connections can be interrupted by a computer's power management setting, which causes it to "go to sleep." The simplest solution to avoid this is to simply reconnect by rerunning the VPN or AOL software, or by re-logging into the secure website.

A second alternative is to change your computer's power management settings so it does not go to sleep; however, this may not be appropriate for portable computers. To change your power management setting under Windows, see the "Power Options" item in the Control Panel.

If you continue to have difficulty with Secure Connections, VPNs, and AOL, please review the steps in the previous pages to be sure you have addressed these issues.

Appendix C: Internet Connection Setting Table

The table on the next page provides references to select and configure Internet connection in setting up your ADSL connection. Many ISPs use different settings depending on the region and equipment they use. You may try the setting for the ISPs in your region. If it does not work, please contact your ISP for your specific setting.

Country	Connection Protocol	VPI/VCI	Encapsulation	ISPs
Europe				
France	PPPoE	8/35	LLC	Various
Germany	PPPoE	1/32	LLC	T-Online, various
Holland	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Various
Belgium	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italy	PPPoE or PPPoA	8/35	VC MUX	TIN
Spain	PPPoE or 1483 Bridged	8/32	LLC	Telefonica
Sweden	1483 Bridged	3/35	LLC	Telia
UK	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Asia				
Australia	PPPoE or PPPoA	8/35	LLC	Various
New Zealand	PPPoE or PPPoA	0/100	VC MUX	Various
Singapore	PPPoE	0/100	LLC	SingNet, Pacific Internet

FCC Statement

DECLARATION OF CONFORMITY WITH FCC RULES FOR ELECTROMAGNETIC COMPATIBILITY

We, Belkin Corporation, of 501 West Walnut Street, Compton, CA 90220, declare under our sole responsibility that the product,

F5D9630-4

to which this declaration relates,
complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: Exposure to Radio Frequency Radiation.
The radiated output power of this device is far below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When connecting an external antenna to the device, the antenna shall be placed in such a manner to minimize the potential for human contact during normal operation. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Federal Communications Commission Notice
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications to this device that are not expressly approved by Belkin Corporation may void the user's authority to operate the equipment.

Canada-Industry Canada (IC)

The wireless radio of this device complies with RSS 139 & RSS 210 Industry Canada. This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Europe-European Union Notice

Radio products with the CE 0560 or CE alert marking comply with the R&TTE Directive (1995/5/EC) issued by the Commission of the European Community.

CE 0560 ⓘ

Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards).

- EN 60950 (IEC60950) – Product Safety
- EN 300 328 Technical requirement for radio equipment
- ETS 300 826 General EMC requirements for radio equipment.

CE ⓘ

To determine the type of transmitter, check the identification label on your Belkin product.

Products with the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage Directive (72/23/EEC) issued by the Commission of the European Community. Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards).

- EN 55022 (CISPR 22) – Electromagnetic Interference
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Electromagnetic Immunity
- EN 61000-3-2 (IEC610000-3-2) – Power Line Harmonics
- EN 61000-3-3 (IEC610000) – Power Line Flicker
- EN 60950 (IEC60950) – Product Safety

CE

Products that contain the radio transmitter are labeled with CE 0560 or CE alert marking and may also carry the CE logo.

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.



Belkin Corporation Limited Lifetime Product Warranty

Belkin Corporation warrants this product against defects in materials and workmanship for its lifetime. If a defect is discovered, Belkin will, at its option, repair or replace the product at no charge provided it is returned during the warranty period, with transportation charges prepaid, to the authorized Belkin dealer from whom you purchased the product. Proof of purchase may be required.

This warranty does not apply if the product has been damaged by accident, abuse, misuse, or misapplication; if the product has been modified without the written permission of Belkin; or if any Belkin serial number has been removed or defaced.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE IN LIEU OF ALL OTHERS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. BELKIN SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

No Belkin dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

BELKIN IS NOT RESPONSIBLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO, LOST PROFITS, DOWNTIME, GOODWILL, DAMAGE TO OR REPROGRAMMING OR REPRODUCING ANY PROGRAM OR DATA STORED IN, OR USED WITH, BELKIN PRODUCTS.

Some states do not allow the exclusion or limitation of incidental or consequential damages or exclusions of implied warranties, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

BELKIN®

ADSL2+ Modem with Wireless G+ MIMO Router

You can find additional support information on our website **www.belkin.com** through the tech-support area.

“If you want to contact technical support by phone, please call the number you need from the list below*. Technical support is available 24 hours a day, 7 days a week.

*National call rates may apply

Free Tech Support*

AUSTRIA	08 - 20 20 07 66	LUXEMBOURG	34 20 80 8560
CZECH REPUBLIC	23 900 04 06	NETHERLANDS	0900 - 040 07 90
DENMARK	701 22 403	NORWAY	815 00 287
FINLAND	00800 - 22 35 54 60	POLAND	00800 - 441 17 37
FRANCE	08 - 25 54 00 26	PORTUGAL	707 200 676
GERMANY	0180 - 500 57 09	RUSSIA	495 580 9541
GREECE	00800 - 44 14 23 90	SOUTH AFRICA	0800 - 99 15 21
HUNGARY	06 - 17 77 49 06	SPAIN	90 - 202 43 66
ICELAND	800 8534	SWEDEN	07 - 71 40 04 53
IRELAND	0818 55 50 06	SWITZERLAND	08 - 48 00 02 19
ITALY	02 - 69 43 02 51	UK	0845 - 607 77 87

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220-5221, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
7 Bowen Crescent, West Gosford
NSW 2250, Australia
+61 (0) 2 4372 8600
+61 (0) 2 4372 8603 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, United Kingdom
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, The Netherlands
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

P75125ea_A

BELKIN®

Modem ADSL2+ avec Routeur Sans Fil G+ MIMO

Reliez vos ordinateurs en réseau et partagez votre connexion Internet ADSL

UK
FR
DE
NL
ES
IT



802.11g
G+
MIMO

Manuel de l'utilisateur

F5D9630fr4A

Table des matières

Merci d'avoir choisi le Modem ADSL avec Routeur Sans Fil G Mode Haut Débit de Belkin (le Routeur). En peu de temps, vous pourrez partager votre connexion Internet et mettre vos ordinateurs en réseau grâce à votre nouveau Routeur. Voici la liste des fonctions qui font de votre Routeur la solution idéale pour vos réseaux domestiques et de petites entreprises. Assurez-vous de lire attentivement ce manuel, particulièrement l'Appendice B intitulée « Facteurs à considérer pour l'installation et la mise en route ».

Les avantages d'un réseau domestique

Grâce à nos instructions pas à pas, votre réseau domestique Belkin vouspermettra de :

- Partager une connexion Internet à haut débit avec tous les ordinateurs de votre domicile
- Partager des ressources, telles que des fichiers et des disques durs, avec tous les ordinateurs de votre domicile
- Partager une imprimante avec toute la famille
- Partager des documents, des fichiers de musique et de vidéo ainsi que des photos numériques
- Stocker, récupérer et copier des fichiers d'un ordinateur à un autre
- Simultanément jouer à des jeux en ligne, consulter une messagerie électronique et discuter

Les avantages d'un réseau sans fil à domicile de Belkin

La Mobilité – nul besoin de confiner votre ordinateur à une seule pièce. Vous pourrez maintenant travailler sur un ordinateur de bureau ou portable, partout dans la zone couverte par votre réseau sans fil

Installation simple – l'Assistant d'Installation de Belkin vous facilite la vie

Polyvalence – accédez à des imprimantes, des ordinateurs ou d'autres périphériques réseau de partout à votre domicile

Possibilité d'expansion – l'étendue de la gamme de produits de mise en réseau offerte par Belkin vous permet d'étendre votre réseau afin d'y inclure des périphériques tels que des imprimantes ou des consoles de jeu

Aucun câblage nécessaire – plus besoin d'effectuer de câblage Ethernet fastidieux et dispendieux

Reconnaissance de l'industrie – choisissez parmi une gamme étendue de produits de mise en réseau interopérables

Assurez-vous de posséder le matériel suivant

Contenu de l'emballage

- Modem ADSL2+ avec Routeur Sans Fil G+ MIMO
- Cordon téléphonique RJ11 - Gris
- Câble réseau Ethernet RJ45 - Jaune
- Micro-filtre ADSL*
- Adaptateur secteur
- Manuel d'utilisation

*Le Micro-filtre ADSL varie d'un pays à l'autre. S'il n'est pas inclus, vous devrez en acheter un.

Configuration requise

- Une connexion ADSL active avec une prise téléphonique pour y brancher le Routeur
- Au moins un ordinateur doté d'une carte d'interface réseau (CIR) et un navigateur Internet installé et configuré
- Protocole réseau TCP/IP installé sur chaque ordinateur relié au Routeur
- Aucun autre serveur DHCP sur votre réseau local assignant des adresses IP aux ordinateurs et aux dispositifs

Paramètres Internet

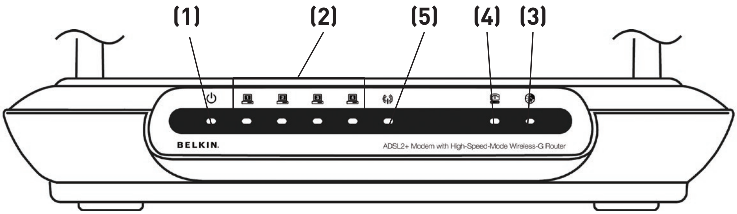
Veuillez obtenir les informations suivantes auprès de votre FAI, avant d'installer votre Modem ADSL avec Routeur Sans Fil G.

- Protocole Internet : ________ (PPPoE, PPPoA, Dynamic IP, Static IP)
- Méthode de multiplexage ou encapsulation : _________ (LLC or VC MUX)
- Circuit virtuel : VPI (Virtual Path Identifier) _________
  (un chiffre entre 0 et 255)
- VCI (Virtual Channel Identifier) _________
  (un chiffre entre 1 et 65535)
- Pour les utilisateurs PPPoE et PPPoA Nom d'utilisateur du compte ADSL _______ ______ et mot de passe ______________
- Pour les utilisateurs IP fixe : Adresse IP ___ . ___ . ___ . ___
  Masque de sous-réseau ___ . ___ . ___ . ___
  Serveur de passerelle par défaut ___ . ___ . ___ .
- Adresse IP du serveur de nom de domaine ___ . ___ . ___ . ___ (si votre FAI vous en a fourni un)

Remarque : Consultez l'Appendice C de ce manuel pour les paramètres Internet ADSL principaux. Dans le doute, contactez votre FAI.

Le Routeur a été conçu pour être placé sur une surface de travail. Tous les câbles sortent de la partie arrière du Routeur, pour une gestion aisée de ceux-ci. Les témoins DEL visibles à l'avant du Routeur vous fournissent des informations sur l'activité et l'état du réseau.

Panneau avant



1. Voyant Alimentation

Lorsque vous mettez le routeur sous tension ou lorsque vous le redémarrez, il se passe un petit laps de temps nécessaire à son amorçage. Une fois que le Routeur a été entièrement initialisé, le témoin d'alimentation est VERT en continu, indiquant que le Routeur est prêt.

	Éteint	Le Routeur est éteint
	Vert	Le Routeur est sous tension
	Rouge	Erreur lors du démarrage du Routeur

2. Témoins de l'état du LAN

Ces témoins portent les numéros 1 à 4 et correspondent aux numéros des ports à l'arrière du Routeur. Lorsqu'un ordinateur est correctement relié à l'un des ports réseau à l'arrière du Routeur, le témoin s'allume. Un témoin vert continu indique une connexion avec ordinateur ou un dispositif réseau. Lorsqu'il y a trafic de données au niveau du port, le témoin clignote rapidement. La couleur ORANGÉ indique une connexion 10Base-T.

	Éteint	Aucun dispositif n'est connecté
	Orangé	Liaison Ethernet avec dispositif 10Base-T
	Orangé - clignotant	Transmission ou réception de données par dispositif 10Base-T
	Vert	Liaison Ethernet avec dispositif 100Base-T
	Vert clignotant	Transmission ou réception de données par dispositif 100Base-T

3. **Témoins d’état WLAN**

Le témoin d’état WLAN est vert continu lorsque vous activez la fonction réseau sans fil LAN. Il clignote lorsque le Routeur transmet ou reçoit des données sans fil.

	Éteint	WLAN est éteint
	Vert	Connexion WLAN en cours
	Vert clignotant	Transmission ou réception de données

4. **Témoin ADSL**

Le témoin ADSL VERT clignote pendant la négociation avec votre FAI. Il demeure VERT lorsque Routeur est correctement branché au service ADSL.

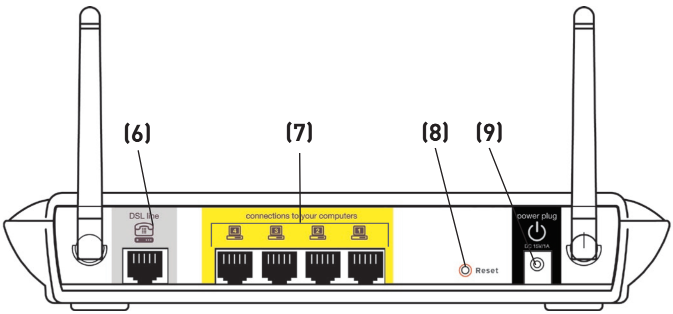
	Éteint	Aucune connexion ADSL
	Vert	Liaison et connexion ADSL actives
	Vert clignotant	Négociation de la connexion

5. **Témoin Internet**

The Internet LED shows you when the Router is connected to the Internet. Quand ce témoin est éteint, le Router N’EST PAS connecté à l’Internet. Quand ce témoin est VERT en continu, le Routeur est connecté à l’Internet. Lorsque ce témoin clignote, le Routeur transmet ou reçoit des données de l’Internet.

	Éteint	Connexion Internet
	Vert	Connecté à l’Internet
	Vert – clignotant	Transmission ou réception de données
	Rouge	Échec lors de l’acquisition de l’adresse IP

Panneau arrière



6. **Ligne ADSL**
   Ce port sert au branchement de votre ligne ADSL. Branchez votre ligne ADSL à ce port.

7. **Ports Ethernet**
   Les ports réseau sont de type RJ45, avec auto-négociation 10/100. Les ports sont numérotés de 1 à 4. Ces ports correspondent aux témoins situés à l'avant du Routeur. Branchez vos ordinateurs ou tout autre périphérique réseau à l'un de ces ports.

8. **Bouton de réinitialisation**
   Le bouton de réinitialisation s'utilise dans les rares cas où votre Routeur fonctionne de façon incongrue. La réinitialisation du Routeur rétablit son fonctionnement normal, tout en conservant les paramètres enregistrés. Vous pouvez aussi rétablir les paramètres par défaut du fabricant à l'aide du bouton de réinitialisation. Vous pouvez utiliser le rétablissement des paramètres par défaut lorsque vous avez oublié votre mot de passe.

   a. **Réinitialisation du Routeur**
      Appuyez sur le bouton « Reset [Réinitialisation] » et maintenez-le enfoncé pendant 1 seconde, puis relâchez-le. Lorsque le témoin Alimentation/Prêt est allumé en continu, la réinitialisation est terminée.

   b. **Rétablissement des paramètres par défaut**
      Appuyez sur le bouton de réinitialisation et maintenez-le enfoncé pendant 5 secondes, puis relâchez-le. Lorsque le témoin « Alimentation/Prêt » est allumé de façon continue, le rétablissement des paramètres est terminé.

9. **Prise d'alimentation**
   Branchez le bloc d'alimentation 15 VCA fourni sur cette prise. L'utilisation de tout autre bloc d'alimentation peut endommager votre Routeur.

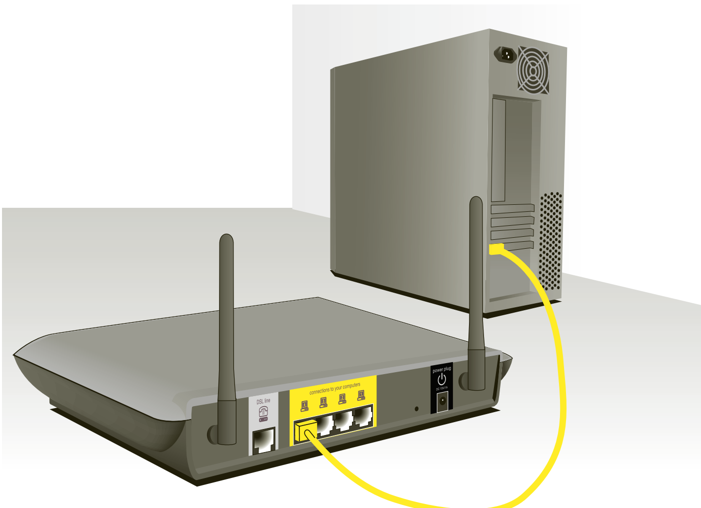
Emplacement de votre Routeur

Plus votre ordinateur se rapproche de votre Point d'Accès ou de votre Routeur, plus votre connexion sans fil gagne en force. De façon générale, la portée de votre réseau sans fil à l'intérieur s'étend de 30 à 60 mètres. À l'opposé, plus vos périphériques sans fil reliés à votre Routeur ou votre Point d'Accès sont éloignés de ceux-ci, moins grande est la performance de votre connexion sans fil. Il se peut que vous vous en rendiez compte ou pas. Si vous éloignez encore plus votre Routeur ou votre Point d'Accès, il est possible que la vitesse de votre connexion diminue. Les appareils électroménagers, les obstacles et les murs peuvent obstruer les signaux radio de votre réseau sans fil et en diminuer la force. Consultez l'Appendice B. Consultez l'Appendice B « Facteurs à considérer pour l'installation et la mise en route » de ce manuel pour en savoir plus.

Dans le but de vérifier si la performance de votre réseau est liée à la portée ou à la présence d'obstacles, déplacez votre ordinateur afin qu'il soit dans un rayon de 2 à 5 mètres du Routeur. Vous verrez ainsi si la distance est la cause des problèmes de performance. Si les problèmes persistent même dans un rayon restreint, consultez la section Dépannage.

Branchement de vos ordinateurs

1. Éteignez votre ordinateur et tous vos dispositifs réseau.
2. Branchez votre ordinateur à l'un des ports RJ45**JAUNES**à l'arrière du Routeur, nommés « connections to your computers [connexion à vos ordinateurs] » au moyen d'un câble réseau Ethernet (un câble réseau Ethernet vous est fourni).



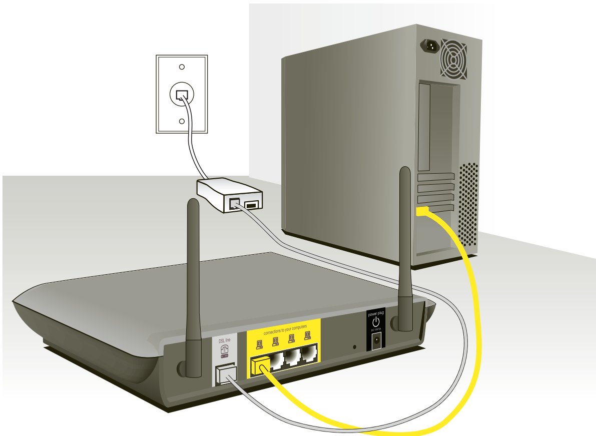
Branchement de l’ADSL

La connexion du Routeur à la ligne ADSL varie selon le pays et la région. De façon générale, la connexion implique un simple filtre ou un filtre avec séparateur intégré, permettant l’utilisation simultanée du service ADSL et du téléphone sur la même ligne téléphonique. Veuillez suivre la procédure ci-dessous selon la méthode appropriée.

1. Si vos services téléphone et ADSL sont sur la même ligne téléphonique, des filtres ADSL sont nécessaires pour chaque téléphone et chaque dispositif, comme les répondeurs, les télécopieurs et les modules d’affichage de l’appelant. Des séparateurs supplémentaires peuvent être utilisés pour séparer les lignes vers le téléphone et le Routeur.

   Remarque : Ne branchez pas le microfiltre ADSL entre la prise murale et le Routeur, ceci empêchera l’acheminement du service ADSL au modem.

2. Si vos services téléphone et ADSL sont sur la même ligne téléphonique et vous utilisez un filtre ADSL avec séparateur intégré, branchez le séparateur à la prise téléphonique murale offrant le service ADSL. Ensuite, branchez le cordon téléphonique du port RJ11 du filtre ADSL, généralement appelé « ADSL », au port RJ11 gris appelé « DSL line [Ligne DSL] » à l’arrière de votre Routeur. Branchez votre appareil téléphonique à l’autre port du séparateur ADSL, généralement appelé « Phone [Téléphone] ». Un filtre ADSL supplémentaire est nécessaire pour tout autre téléphone ou appareil se trouvant sur la même ligne.



Remarque : Un cordon téléphonique RJ11 est fourni. Lorsque vous insérez une fiche RJ11, assurez-vous que l'onglet de la fiche s'enclenche pour garantir une bonne fixation.

3. Si vous possédez une ligne téléphonique avec service ADSL dédié via une prise murale RJ11, branchez simplement un cordon téléphonique de la prise murale vers le port RJ11 gris appelé « DSL line [Ligne ADSL] » à l'arrière du Routeur.

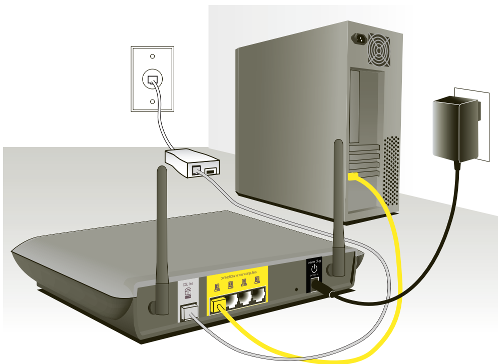
4. Si vous recevez votre service ADSL par une prise murale RJ45, branchez un adaptateur RJ45/RJ11 sur la prise murale. Branchez ensuite une extrémité du cordon téléphonique à l'adaptateur et l'autre extrémité au port gris RJ11 appelé « DSL line [Ligne ADSL] » à l'arrière du Routeur.

   Remarque : Le filtre ADSL peut vous être fourni ou non, selon votre pays.

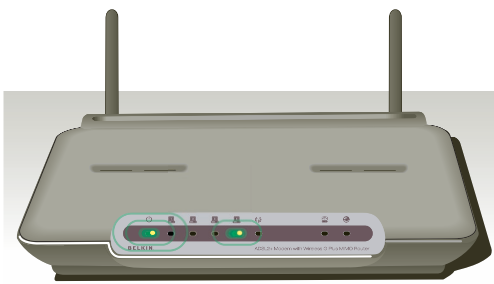
Mise en marche du Routeur

1. Branchez le bloc d'alimentation fourni dans la prise d'alimentation du Routeur.

   Remarque : Pour une meilleure performance, une sécurité optimale et éviter d'endommager le Routeur, n'utilisez que l'adaptateur fourni.



2. Après avoir branché l'adaptateur de courant et mis le Routeur sous tension, le témoin d'alimentation du Routeur ⏻ doit être allumé. Le démarrage complet du Routeur peut prendre plusieurs minutes.



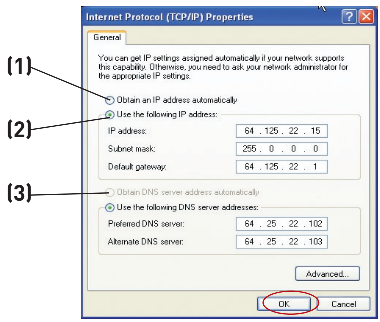
3. Allumez vos ordinateurs. Une fois les ordinateurs amorcés, un témoin LAN 💻 (à l'avant du Routeur), correspondant à chaque port auquel un ordinateur câblé est connecté, s'allume. Ces témoins indiquent l'état de la connexion et l'activité. Vous êtes maintenant prêt à configurer le Routeur en vue de la connexion au service ADSL.

Afin que votre ordinateur soit en mesure de communiquer avec votre Routeur, vous devez vous assurer que les paramètres TCP/IP Ethernet soient à « Obtain an IP address automatically/Using DHCP [Obtenir une adresse IP automatiquement/Utiliser serveur DHCP] ». C'est le paramètre par défaut de la plupart des ordinateurs domestiques.

Procédez comme suit pour configurer D'ABORD l'ordinateur connecté au modem ADSL. Vous pouvez également suivre les étapes suivantes pour ajouter des ordinateurs à votre Routeur après que celui-ci soit configuré pour accéder à l'Internet.

Configuration manuelle des paramètres réseau sous Windows XP, 2000 ou NT

1. Cliquez sur « Démarrer », « Paramètres » puis « Panneau de Configuration ».
2. Cliquez deux fois sur l'icône « Network and dial-up connections [Connexions réseau et accès à distance] » (Windows 2000) ou sur l'icône « Network [Réseau] » (Windows XP).
3. Cliquez avec le bouton droit de la souris sur la connexion au réseau local associée à votre carte réseau, puis sélectionnez « Properties [Propriétés] » dans le menu déroulant.



4. Dans la fenêtre « Local Area Connection Properties [Propriétés de la connexion au réseau local] », sélectionnez « Internet Protocol (TCP/IP) [Protocole Internet (TCP/IP] », puis cliquez sur le bouton « Properties [Propriétés] ». L'écran suivant apparaît :
5. Si l'option « Use the following IP address [Utiliser l'adresse IP suivante] » **(2)** est sélectionnée, votre Routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le Routeur.

IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

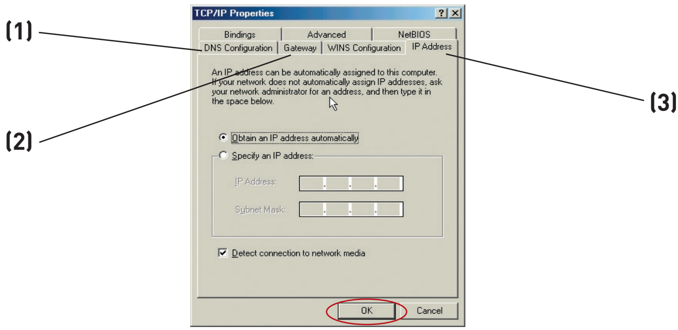
6. Si elles ne sont pas déjà sélectionnées, choisissez les options « Obtain an IP address automatically [Obtenir automatiquement une adresse IP] » **(1)** et « Obtain DNS server address automatically [Obtenir les adresses des serveurs DNS automatiquement] » **(3)**. Cliquez sur « OK ».

Votre(vos) adaptateur(s) réseau est(sont) maintenant configuré(s) de manière à fonctionner avec le Routeur.

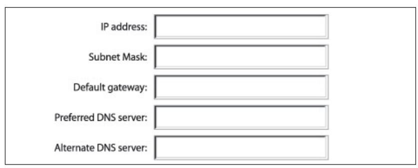
Configuration manuelle des adaptateurs réseau sous Windows 98SE ou Me

1. Cliquez avec le bouton droit de la souris sur « Network Neighborhood [Voisinage réseau] » et sélectionnez « Properties [Propriétés] » dans le menu déroulant.

2. Sélectionnez « TCP/IP -> settings [TCP/IP -> paramètres] » pour la carte réseau installée. Vous verrez l'écran suivant.



3. Si l'option « Specify an IP address [Spécifier une adresse IP] » est sélectionnée, votre Routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le Routeur.



4. Écrivez l'adresse IP et le masque de sous-réseau de l'onglet « IP Address [Adresse IP] »**(3)**.

5. Cliquez sur l'onglet « Gateway [Passerelle] » **(2)**. Notez l'adresse de la passerelle dans le tableau.

6. Cliquez sur l'onglet « DNS Configuration [Configuration DNS] » **(1)**. Inscrivez les adresses DNS dans le tableau.

7. Si elle n'est pas déjà sélectionnée, choisissez l'option « Obtain IP address automatically [Obtenir automatiquement une adresse IP] » sur l'onglet des adresses IP. Cliquez sur « OK ».

8. Vous devrez également supprimer l'adresse de passerelle de l'onglet Passerelle et les entrées de configuration DNS afin de configurer la connexion de votre Routeur Belkin.

Redémarrez l'ordinateur. Lorsque l'ordinateur redémarre, votre(vos) adaptateur(s) réseau est(sont) maintenant configuré(s) de manière à fonctionner avec le Routeur.

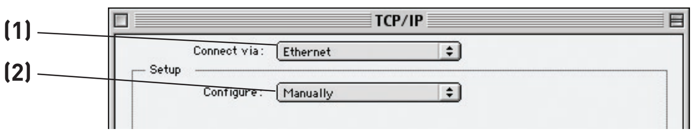
Procédez comme suit pour configurer D'ABORD l'ordinateur connecté au modem câble ou ADSL. Vous pouvez aussi suivre les étapes suivantes pour ajouter des ordinateurs à votre Routeur après que celui-ci est configuré pour accéder à l'Internet.

Configuration manuelle des paramètres réseau sous Mac OS jusqu'à 9.x

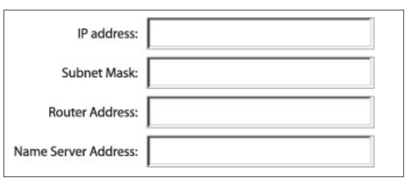
Afin que votre ordinateur puisse communiquer efficacement avec votre Routeur, vous devrez modifier les paramètres TCP/IP de votre Mac à DHCP.

1. Déroulez le menu Pomme. Sélectionnez « Control Panels [Tableaux de bord] », puis « TCP/IP».

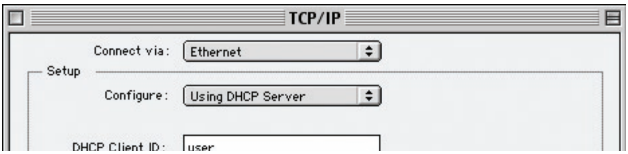
2. Vous verrez le tableau de bord TCP/IP. Sélectionnez « Ethernet Built-In [Ethernet intégré] » ou « Ethernet » dans le menu déroulant « Connect via: [Connecter via :] » **(1)**.



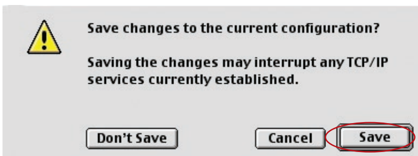
3. À côté de « Configure [Configurer] » **(2)**, si l'option « Manually [Manuellement] » est sélectionnée, votre Routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le Routeur.



4. Si cela n'est pas déjà fait, au niveau de « Configure [Configurer] », choisissez « Using DHCP Server [Utiliser le serveur DHCP] ». Ceci permet d'indiquer à l'ordinateur qu'il doit obtenir une adresse IP auprès du Routeur.



5. Fermez la fenêtre. Si vous avez apporté des modifications, la fenêtre suivante apparaît. Cliquez sur « Save [Enregistrer] ».



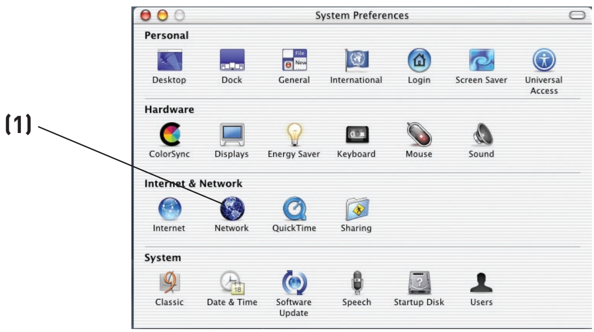
Redémarrez l'ordinateur. Lorsque l'ordinateur redémarre, vos paramètres réseau sont maintenant configurés de manière à fonctionner avec le Routeur.

Configuration manuelle des Adaptateurs réseau sous Mac OS X

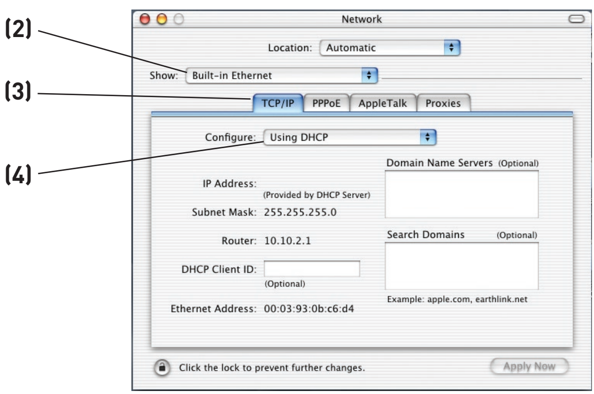
1. Cliquez sur l’icône « System Preferences [Préférences système] ».



2. Sélectionnez « Network [Réseau] »**(1)**à partir du menu « System Preferences [Préférences du système] ».

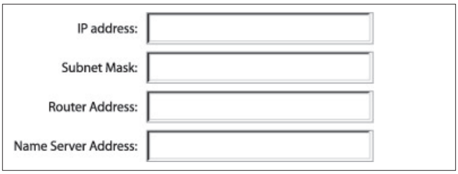


3. Selectionnez « Built-in Ethernet [Ethernet intégré] » **(2)** à côté de « Show [Montrer] », dans le menu « Network [Réseau] ».



4. Sélectionnez l'onglet « TCP/IP » **(3)**. À côté de « Configure [Configurer] » **(4)**, vous devriez voir « Manually [Manuellement] » ou « Using DHCP [Utiliser DHCP] ». Si tel n'est pas le cas, vérifiez dans l'onglet « PPPoE » **(5)** que l'option « Connect using PPPoE [Se connecter via PPPoE] » n'est PAS sélectionnée. Si c'est le cas, vous devrez configurer votre Routeur pour une connexion de type PPPoE, utilisant votre nom d'utilisateur et mot de passe.

5. Si l'option « Manually [Manuellement] » est sélectionnée, votre Routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le Routeur.

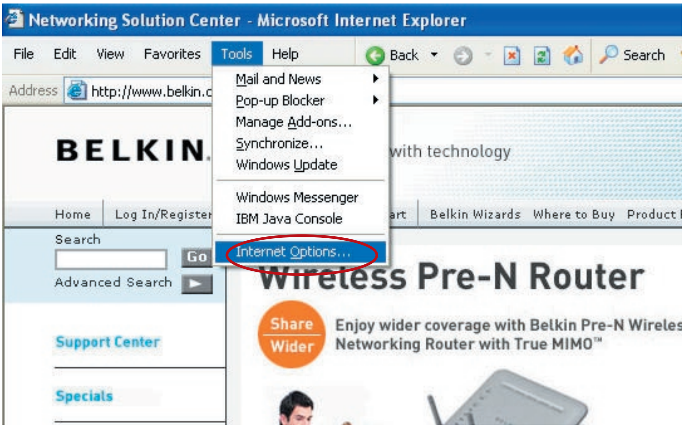


6. Si cela n'est pas déjà fait, sélectionnez « Using DHCP [Via DHCP] » à côté de « Configure [Configurer] » **(4)**, puis cliquez sur « Apply Now [Appliquer maintenant] ».

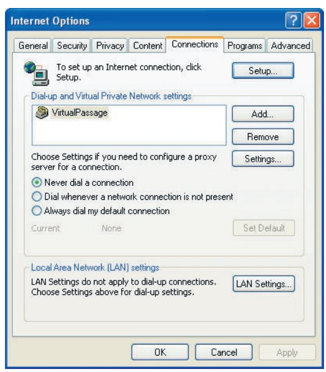
Votre(vos) adaptateur(s) réseau est(sont) maintenant configuré(s) de manière à fonctionner avec le Routeur.

Paramètres de navigateur recommandés

La plupart du temps, vous n'aurez pas besoin de modifier les paramètres de votre navigateur Web. Si vous rencontrez des problèmes pour accéder à Internet ou avec l'interface utilisateur évoluée basée sur le Web, modifiez les paramètres de votre navigateur et choisissez ceux conseillés dans cette section.

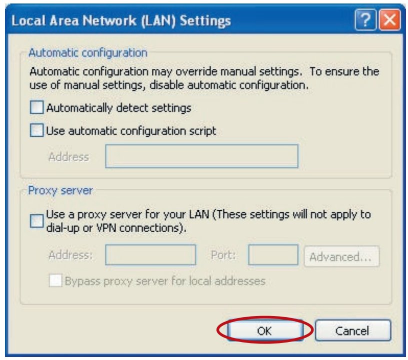


Internet Explorer 4.0 ou version ultérieure



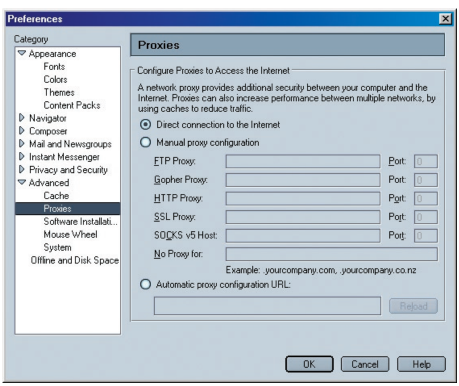
1. Lancez votre navigateur Web. Dans le menu « Tools [Outils] », sélectionnez la commande « Internet Options [Options Internet] ».
2. À l'écran « Internet Options [Options Internet] », trois choix sont possibles : « Never dial a connection [Ne jamais établir de connexion] », « Dial whenever a network connection is not present [Établir une connexion s'il n'existe pas de connexion réseau] » et « Always dial my default connection [Toujours établir la connexion par défaut] ». Si vous le pouvez, sélectionnez l'option « Never dial a connection [Ne jamais établir de connexion] ». Si vous ne pouvez pas, passez à l'étape suivante.
3. À l'écran « Internet Options [Options Internet] », cliquez sur « Connections [Connexions] », puis sélectionnez « LAN Settings... [Paramètres du réseau local] ».

4. Assurez-vous qu'aucune de ces options n'est cochée : « Automatically detect settings [Détecter automatiquement les paramètres de connexion] », « Use automatic configuration script [Utiliser un script de configuration automatique] » et « Use a proxy server [Utiliser un serveur proxy] ». Cliquez sur « OK ». Ensuite, cliquez de nouveau sur « OK » à la page « Internet Options [Options Internet] ».



Netscape Navigator 4.0 ou version ultérieure

1. Lancez Netscape. Dans le menu « Edit [Edition] », cliquez sur « Preferences [Préférences] ».
2. Dans la fenêtre « Preferences [Préférences] », cliquez sur « Advanced [Avancé] », puis sélectionnez « Proxies [Serveurs proxy] ». Dans la fenêtre « Proxies [Serveurs proxy] », sélectionnez « Direct connection to the Internet [Connexion directe à Internet] ».



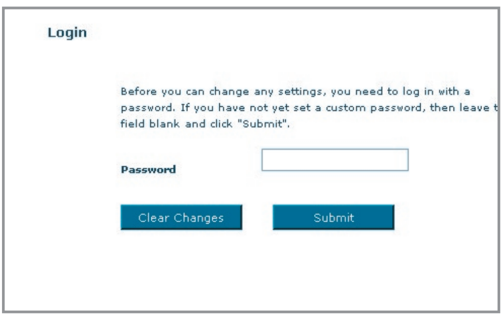
Lancement de l’Assistant

1. Vous pouvez accéder à l’interface-utilisateur basée sur le Web du Routeur à l’aide d’un navigateur, à partir d’un ordinateur physiquement connecté au Routeur. Dans la barre d’adresse, tapez 192.168.2.254 » (ne tapez pas les http:// ou www). Appuyez ensuite sur la touche « Entrée ».



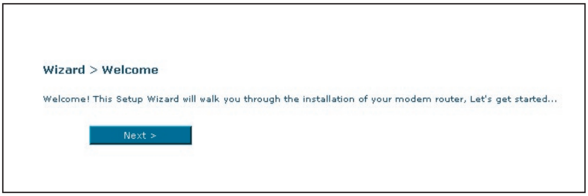
Remarque : Nous vous recommandons fortement d’utiliser un ordinateur directement relié au Routeur par un câble RJ45 pour la configuration initiale. L’utilisation d’un ordinateur relié au Routeur par une connexion sans fil n’est pas recommandée.

2. L’écran suivant apparaît dans votre navigateur, vous invitant à vous connecter. Le Routeur est livré sans mot de passe. À l’écran de connexion, laissez le mot de passe vide et cliquez sur le bouton « Submit [Envoyer] » pour vous connecter.

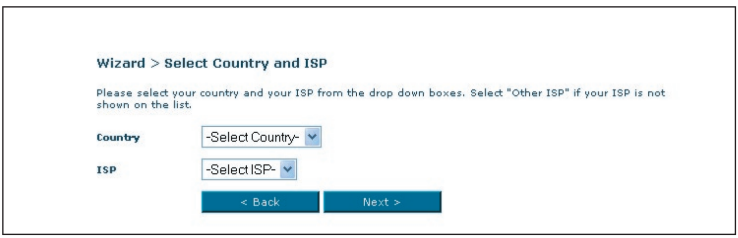


Remarque : Pour plus de sécurité, nous vous conseillons vivement de définir votre mot de passe administrateur. Veuillez lire le Manuel de l’Utilisateur pour de plus amples détails sur comment changer votre mot de passe et connaître d’autres fonctions de sécurité.

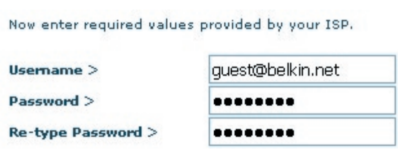
3 L'Assistant démarre automatiquement avec la configuration express (recommandé). Cliquez sur « Next [Suivant] » pour poursuivre.



4 Tout d'abord, sélectionnez votre pays et votre FAI, puis cliquez sur « Next [Suivant] ». Si votre pays et/ou votre FAI ne figurent pas dans la liste, sélectionnez « Other Country [Autre pays] » ou «Other ISP [Autre FAI] ».



5 Entrez le nom d'utilisateur et le mot de passe fourni par votre Fournisseur d'Accès à Internet (FAI) dans les champs vides. Le nom d'utilisateur et le mot de passe doivent être valides, sinon la connexion ne peut s'effectuer. Votre FAI est en mesure de confirmer votre nom d'utilisateur et votre mot de passe.



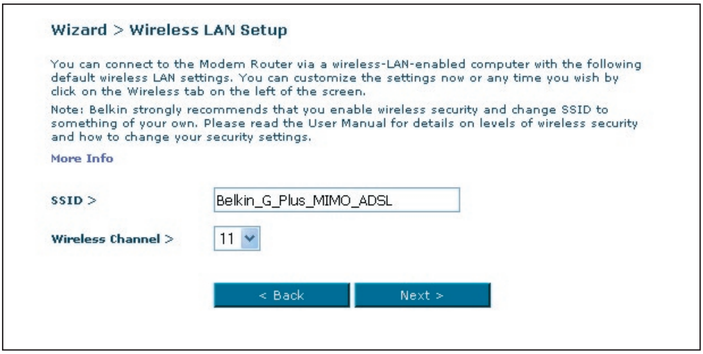
Remarque : Pour en savoir plus à propos des autres types de connexion, consultez la section « Configuration manuelle du Routeur » de ce manuel.

6 L'écran d'implémentation du réseau sans fil apparaît. Vous pouvez maintenant vous connecter au Routeur à partir d'un ordinateur doté d'un dispositif réseau sans fil, à l'aide des paramètres par défaut suivants :

SSID = Belkin G+ MIMO ADSL

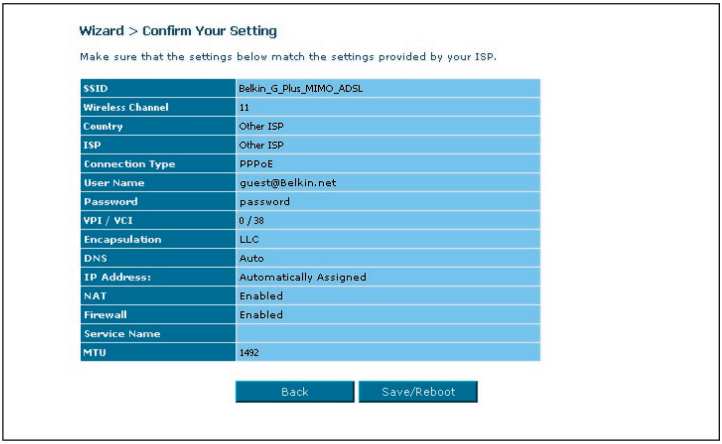
Canal sans fil = Auto

Sécurité = off [Désactivé]



Remarque : Belkin vous recommande fortement d'activer une fonction de sécurité (WEP ou WPA) et de modifier le SSID pour qu'il soit unique à votre réseau. Consultez le Manuel de l'Utilisateur pour connaître les niveaux de sécurité et comment modifier vos paramètres de sécurité.

7. Vérifiez les paramètres montrés à l'écran suivant. Cliquez sur « Back [Précédent] » pour modifier les paramètres ou cliquez « Apply [Appliquer] » pour confirmer.


Wizard > Confirm Your Setting

Make sure that the settings below match the settings provided by your ISP.

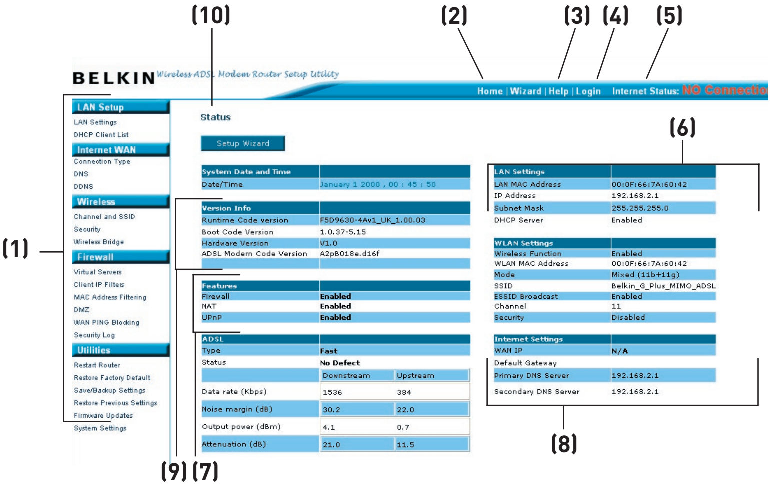
SSID	Belkin_G_Plus_MIMO_ADSL
Wireless Channel	11
Country	Other ISP
ISP	Other ISP
Connection Type	PPPoE
User Name	guest@Belkin.net
Password	password
VPI / VCI	0 / 38
Encapsulation	LLC
DNS	Auto
IP Address:	Automatically Assigned
NAT	Enabled
Firewall	Enabled
Service Name	
MTU	1492

Back Save/Reboot

Remarque : Vous pouvez en tout temps redémarrer l'Assistant de Configuration ou utiliser le Menu de Navigation à gauche pour modifier vos paramètres.

Faites connaissance avec l'interface-utilisateur basée sur navigateur Web

La page d'accueil vous montre un aperçu de l'état du Routeur et de ses paramètres. À partir de cette page, vous pouvez rejoindre toutes les pages ayant trait à la configuration.



1. **Raccourcis de navigation**
Vous pouvez passer à n'importe quelle autre page de l'IU en cliquant directement sur ces raccourcis. Les raccourcis sont classés par catégories et groupés à l'aide d'onglets pour faciliter l'accès à un paramètre particulier. En cliquant sur le titre de chaque onglet, vous verrez une courte description des fonctions classées sous cet onglet.

2. **Bouton Accueil**
Le bouton « Accueil » est disponible à chaque page de l'IU. En cliquant sur ce bouton, vous retournez à la page d'accueil.

3. **Bouton Aide**
Le bouton « Aide » vous permet d'accéder aux pages d'aide du Routeur. Vous pouvez également obtenir de l'aide sur de nombreuses pages. Pour cela, cliquez sur « More info [Plus d'infos] » en regard de certaines sections de chaque page.

4. **Bouton Connexion/Déconnexion**
Ce bouton vous permet d'ouvrir ou de fermer une session sur le Routeur en appuyant sur un bouton. Lorsque vous êtes connecté au

Routeur, ce bouton indique « Logout [Déconnexion] ». La connexion au Routeur vous transportera vers une page de connexion séparée, où vous devrez entrer un mot de passe. Lorsque vous êtes connecté au Routeur, vous pouvez apporter des modifications aux paramètres. Une fois les modifications apportées, vous pouvez vous déconnecter du Routeur. Pour cela, cliquez sur le bouton « Logout [Déconnexion] ». Pour plus d'informations sur la connexion au Routeur, reportez-vous à la section « Connexion au Routeur ».

5. **Indicateur de l'état de l'Internet**

   Cet indicateur est visible sur toutes les pages du Routeur, et montre l'état de la connexion du Routeur. Lorsqu'il indique « connection OK [Connexion OK] » en VERT, le Routeur est connecté à Internet. Lorsque le Routeur n'est pas connecté à Internet, l'indicateur affiche « No connection [Pas de connexion] » en ROUGE. Lorsque vous apportez des modifications aux paramètres du Routeur, l'indicateur est mis à jour automatiquement.

6. **Paramètres LAN**

   Montre les réglages du côté du réseau local (Local Area Network - LAN) du Routeur. Vous pouvez apporter des modifications aux paramètres en cliquant sur le raccourci de navigation « LAN » à la gauche de l'écran.

7. **Fonctions**

   Montre l'état de la NAT, du pare-feu et des fonctions sans fil du Routeur. Pour modifier ces paramètres, cliquez sur l'un des liens ou sur le lien de navigation rapide sur la partie gauche de l'écran.

8. **Paramètres Internet**

   Indique les paramètres Internet/WAN du Routeur connecté à l'Internet. Vous pouvez modifier les paramètres en cliquant sur le raccourci de navigation « Internet/WAN » à la gauche de l'écran.

9. **Information sur la version**

   Montre les versions du micrologiciel, du code de démarrage, du matériel, ainsi que le numéro de série du Routeur.

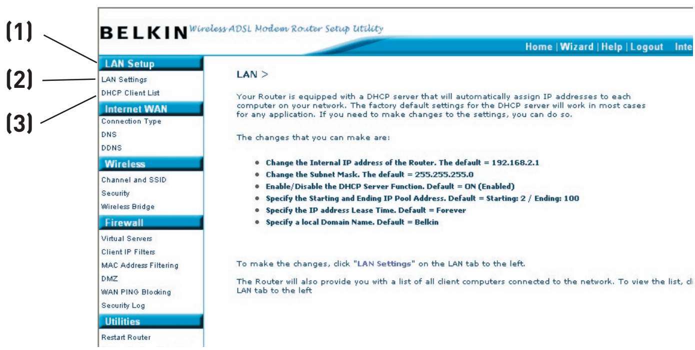
10. **Nom de la page**

    La page sur laquelle vous vous trouvez peut être identifiée par ce nom. Ce manuel réfère parfois au nom de ces pages. Par exemple, «LAN > LAN Settings [LAN > Paramètre LAN] » réfère à la page « LAN Settings [Paramètres LAN] ».

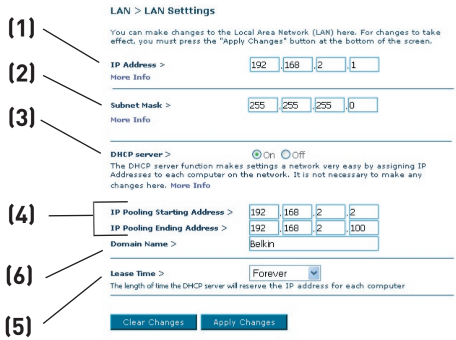
Modification des paramètres de réseau local (LAN)

Tous les paramètres de réseau local (LAN) du Routeur peuvent être visualisés et modifiés ici.

Pour accéder à page d'accueil de l'onglet LAN (réseau local) **(1)**, cliquez sur le titre de celui-ci. Vous y trouverez une courte description des fonctions. Pour afficher les paramètres ou modifier n'importe quel de ces paramètres de réseau local, cliquez sur « LAN Settings [Paramètres de réseau local] »**(2)** ou pour afficher la liste des ordinateurs connectés, cliquez sur « DHCP Client List [Liste des clients DHCP] » **(3)**.



Paramètres de réseau local



1. **Adresse IP**

   L' « Adresse IP » représente l'Adresse IP interne du Routeur. L'adresse IP par défaut est 192.168.2.1. Pour accéder à l'interface de configuration avancée, entrez cette adresse IP dans la barre d'adresse de votre navigateur. Cette adresse peut être modifiée au besoin. Pour modifier l'adresse IP, entrez la nouvelle adresse IP et cliquez sur « Apply Changes [Enregistrer les Modifications] ». L'adresse IP choisie doit être une adresse IP non-acheminable. Exemples d'adresses IP non-acheminables :

   192.168.x.x (où x est un nombre compris entre 0 et 255.)

   110.x.x.x (où x est un nombre compris entre 0 et 255.)

2. **Masque de sous-réseau**

   Il n'est pas nécessaire de modifier le masque de sous-réseau, puisque le Routeur en ajuste la longueur automatiquement selon le type d'adresse IP.

3. **Serveur DHCP**

   Le serveur DHCP rend la mise en oeuvre d'un réseau très simple, en attribuant automatiquement des adresses IP à tous les ordinateurs du réseau. La valeur par défaut est « ON [Activé] ». La fonction de serveur DHCP peut être désactivée si nécessaire. Toutefois, si vous désactivez le Serveur DHCP, vous devrez entrer manuellement une adresse IP statique pour chacun des ordinateurs de votre réseau. Pour désactiver le serveur DHCP, sélectionnez l'option « Off [Désactivé] », puis cliquez sur « Apply Changes [Enregistrer les modifications] ».

4. **Réserve IP**

   La réserve IP est la plage d'adresses IP mises de côté pour attribution dynamique aux ordinateurs faisant partie de votre réseau. La valeur par

défaut est de 2 à 100 (c'est à dire 99 ordinateurs). Pour changer ce nombre, entrez de nouvelles adresses IP de début et de fin, puis cliquez sur « Apply Changes [Enregistrer les modifications] ». Le serveur DHCP peut assigner automatiquement 100 adresses IP. Ceci veut dire que vous ne pouvez pas spécifier une réserve d'adresses IP supérieure à 100 ordinateurs. Par exemple, si l'adresse de départ est 50, l'adresse d'arrivée doit être 150 (ou inférieure), afin de ne pas surpasser la limite de 100 clients. L'adresse IP de départ doit être inférieure en nombre à l'adresse IP d'arrivée.

5. **Durée d'autorisation**

   La durée pendant laquelle le serveur DHCP réservera l'adresse IP pour chaque ordinateur. Nous vous conseillons de laisser la durée d'autorisation à « Forever [Toujours] ». La valeur par défaut est « Forever [Toujours] », ce qui signifie que chaque fois que le serveur DHCP attribue une adresse IP à un ordinateur, cette adresse ne changera pas pour l'ordinateur. Entrer une durée d'autorisation plus courte, comme un jour ou une heure, libère les adresses IP après l'intervalle de temps donné. Ceci veut en outre dire que l'adresse IP d'un ordinateur peut changer au fil du temps. Si vous avez configuré quelques-unes des fonctions avancées du Routeur, telles que la zone DMZ ou le filtre d'adresses IP des clients, rappelez-vous que ces paramètres dépendent d'une adresse IP spécifique. Ainsi, il serait préférable que l'adresse IP demeure la même.

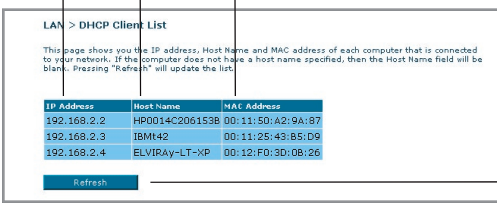
6. **Nom de Domaine local**

   Le paramètre par défaut est « Belkin ». Vous pouvez donner un nom de domaine local (nom de réseau) à votre réseau. Il n'est pas nécessaire de modifier ce paramètre à moins qu'un impératif particulier ne vous y oblige. Vous êtes libre de donner le nom de votre choix à votre réseau, comme par exemple Mon Réseau .

Liste de Clients DHCP

Vous pouvez visualiser une liste d'ordinateurs (appelés « clients ») connectés à votre réseau. Vous êtes en mesure de visualiser l'adresse IP **(1)** de l'ordinateur, le nom d'hôte **(2)** (si l'ordinateur s'en est vu attribuer un), et l'adresse MAC **(3)** de la carte d'interface réseau de cet ordinateur. Cliquez sur le bouton « Refresh [Actualiser] » **(4)** pour mettre la liste à jour. La liste est mise à jour s'il y a eu un quelconque changement.

(1) **(2)** **(3)**



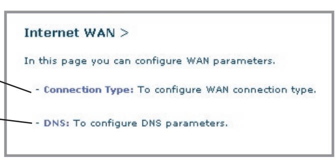
(4)

Internet / WAN

L'onglet « Internet/WAN » est l'endroit où vous allez configurer le Routeur pour qu'il se connecte chez votre Fournisseur d'Accès à Internet (FAI). Le Routeur peut se connecter pratiquement à n'importe quel système ADSL offerts par un FAI, si bien sûr vous avez configuré votre Routeur avec les paramètres appropriés au type de connexion de votre FAI. Vos paramètres de connexion vous sont fournies par votre FAI. Pour configurer le Routeur avec les paramètres fournis par le FAI, cliquez sur « Connection Type [Type de connexion] » **(1)** sur le côté gauche de l'écran. Sélectionnez votre type de connexion. Si votre FAI vous a fourni des paramètres DNS, cliquez sur « DNS » **(2)** pour entrer l'adresse DNS de votre FAI qui nécessite des paramètres particuliers.

Lorsque vous avez terminé d'apporter ces modifications, l'indicateur « Internet Status [État de l'Internet] » affiche « Connection OK [Connexion OK] » si le Routeur a été correctement configuré.

(1)
(2)



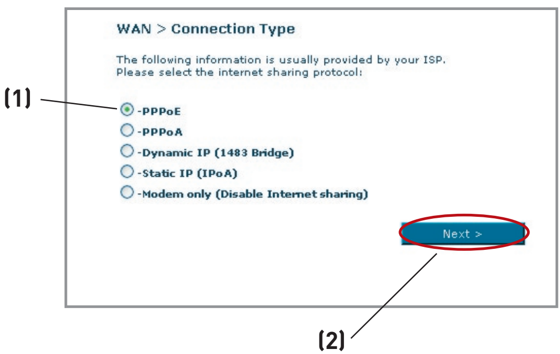
Type de Connexion

À la page « Connection Type [Type de connexion] », vous pouvez choisir l'un des cinq types de connexions, selon les informations fournies par votre FAI :

- PPPoE
- PPPoA
- IP Dynamique (1483 Bridged)
- IP fixe (IPOA)
- Modem seulement (désactivation du partage de l'Internet)

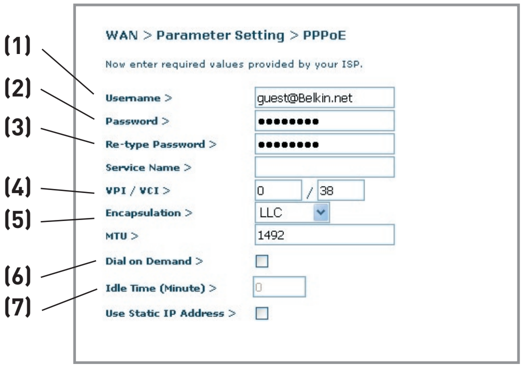
Remarque : Consultez l'Appendice C de ce manuel pour les paramètres Internet ADSL principaux. En cas de doute, contactez votre FAI.

Cliquez sur le bouton radio **(1)** en regard du type de connexion, puis cliquez sur « Next [Suivant] »**(2)**



Configuration de votre connexion de type PPPoE ou PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) est la méthode de connexion standard pour les dispositifs réseau. Elle requiert un nom d'utilisateur et un mot de passe pour accéder au réseau de votre FAI, pour vous connecter à l'Internet. Le PPPoA (PPP over ATM) est similaire au PPPoE, mais se retrouve plutôt au Royaume-Uni. Sélectionnez PPPoE ou PPPoA et cliquez sur « Next [Suivant] ». Entrez ensuite les informations fournies par votre FAI, puis cliquez « Apply Changes [Enregistrer les modifications] » pour activer les paramètres.



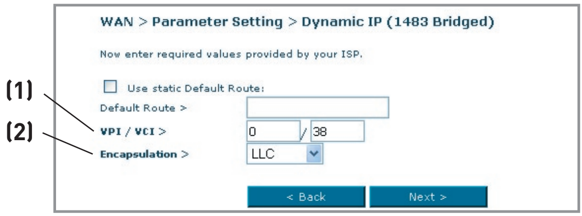
1. **Nom d'utilisateur-** Entrez le nom d'utilisateur. (Fourni par votre FAI.)
2. **Mot de passe -** Entrez votre mot de passe. (Fourni par votre FAI.)
3. **Entrez à nouveau le mot de passe -** Confirmer le mot de passe. (Fourni par votre FAI.)
4. **VPI/VCI -** Entrez ici vos paramètres de d'identificateur de trajet virtuel (VPI) et d'identificateur de voie virtuelle (VCI). (Fourni par votre FAI.)
5. **Encapsulation -** Sélectionnez votre type d'encapsulation (fourni par votre FAI) afin de spécifier comment traiter les protocoles multiples sur la couche de transport ATM.

   VC-MUX : Le PPPoA Virtual Circuit Multiplexer (null encapsulation) ne permet qu'un seul protocole par circuit virtuel, avec moins de surdébits.

   LLC : Le PPPoA Logical Link Control permet plusieurs protocoles sur un circuit virtuel (plus de surdébit).
6. **Dial on Demand [Numérotation à la demande] -** Si vous sélectionnez « Dial on Demand », votre Routeur se connecte à l'Internet lorsqu'un utilisateur lance un navigateur Web.
7. **Idle Time (minutes) [Temps d'inactivité] -** Entrez le temps d'inactivité maximum de la connexion à Internet. Lorsque cet intervalle de temps est dépassé, la connexion à Internet prend fin.

Configuration de votre type de connexion avec IP Dynamique (1483 Bridged)

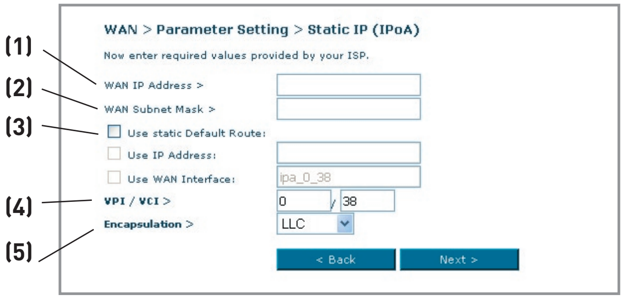
Cette méthode de connexion relie votre réseau et le réseau de votre FAI. Le Routeur obtienr une adresse IP automatiquement du serveur DHCP de votre FAI.



1. **VPI/VCI -** Entrez ici vos paramètres de d'identificateur de trajet virtuel (VPI) et d'identificateur de voie virtuelle (VCI). Ces identifiants vous sont fournis par votre FAI.
2. **Encapsulation -** Sélectionnez LLC ou VC MUX, selon le paramètre de votre FAI.

Réglage du type de connexion FAI comme ‘ IP fixe ‘ (IPoA)

Ce type de connexion est également appelé « Classical IP over ATM [IP Classique sur ATM] » ou « CLIP », où votre FAI vous attribue une adresse IP fixe pour la connexion du Routeur à l’Internet.

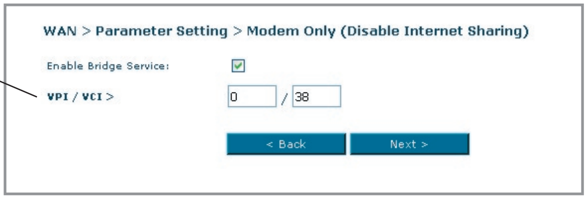


1. **Adresse IP WAN –** Entrez une adresse IP fournir par votre FAI pour l’interface WAN du Routeur.
2. **Masque de sous-réseau WAN -** Entrez un masque de sous-réseau fourni par votre FAI.
3. **Route par défaut -** Entrez une adresse IP de passerelle par défaut. Si le Routeur ne peut trouver l’adresse de destination au sein de son réseau local, il relaiera les paquets de données vers la passerelle par défaut fournie par votre FAI.
4. **VPI/VCI -** Entrez ici vos paramètres de d’identificateur de trajet virtuel (VPI) et d’identificateur de voie virtuelle (VCI). Ces identifiants vous sont fournis par votre FAI.
5. **Encapsulation -** Sélectionnez LLC ou VC MUX, selon le paramètre de votre FAI.

Configuration de votre connexion à Modem uniquement (désactivation du partage de l'Internet)

Dans ce mode, le Routeur agit en tant que simple passerelle pour les paquets de données transitant sur le port DSL. Vous devez également installer des logiciels supplémentaires sur votre ordinateur pour accéder à l'Internet.

(1)

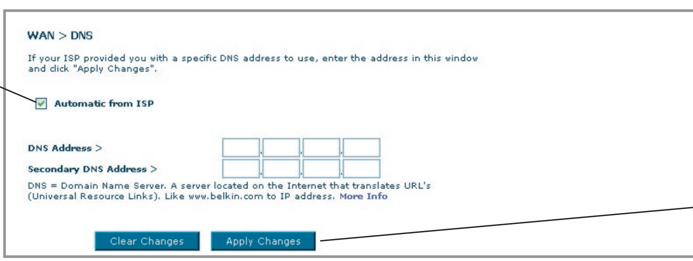


1. VPI/VCI - Entrez ici vos paramètres de d'identificateur de trajet virtuel (VPI) et d'identificateur de voie virtuelle (VCI). (Fourni par votre FAI.)

Paramètres DNS (Domain Name Server - serveur de nom de domaine)

Un Serveur de Noms de Domaine est un serveur que l'on retrouve sur l'Internet et qui traduit les URL (Universal Resource Links), telles que www.belkin.com, en adresses IP. Cette information n'est pas requise de la plupart des FAI lors de la configuration du Routeur. La case « Automatic from ISP [Obtenir automatiquement du FAI] » **(1)** doit être cochée si votre FAI ne vous a pas fourni d'adresse DNS particulière. Si vous êtes utilisez une connexion de type IP statique, vous pouvez avoir besoin de saisir une adresse DNS spécifique ainsi qu'une adresse DNS secondaire pour que votre connexion puisse fonctionner correctement. Si vous utilisez une connexion de type dynamique ou PPPoE, il est fort probable que vous n'ayez pas à entrer une adresse de DNS. Laissez la case « Automatic from ISP [Obtenir automatiquement du FAI] » cochée. Pour entrer les paramètres d'adresse DNS, désélectionnez la case « Automatic from ISP [Obtenir automatiquement du FAI] » et entrez les numéros DNS dans les espaces fournis à cet effet. Cliquez sur « Apply changes [Enregistrer les modifications] »**(2)** pour enregistrer les paramètres.

(1)



(2)

Utilisation du serveur DNS dynamique

Le service DNS Dynamique vous permet d'attribuer une adresse IP dynamique à un nom d'hôte statique parmi ceux offerts par DynDNS.org, ce qui vous permet d'accéder à vos ordinateurs à partir de maints endroits sur Internet. DynDNS.org offre ce service à la communauté des Internautes, gratuitement, pour jusqu'à cinq noms d'hôte.

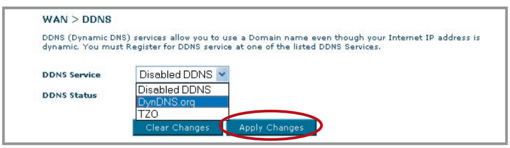
Le service DNS Dynamique est idéal pour les sites web maison, les serveurs de fichiers, ou pour vous faciliter l'accès à votre PC ou aux fichiers stockés sur votre PC lorsque vous êtes au boulot. Le service garantit que votre nom d'hôte pointe toujours vers votre adresse IP, peut importe si votre FAI modifie celle-ci. Lorsque votre adresse IP change, vos amis et associés peuvent toujours vous retrouver en visitant votrenom.dyndns.org !

Inscrivez-vous gratuitement et obtenez votre nom d'hôte DNS Dynamique à http://www.dyndns.org.

Configuration du client DNS Dynamique du Routeur

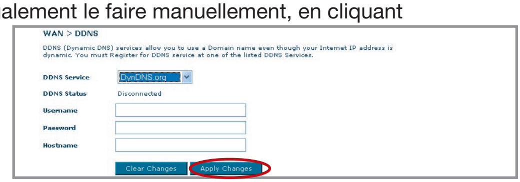
Vous devez vous inscrire au service gratuit de mise à jour de DynDNS.org avant d'utiliser cette fonction. Après vous être inscrit, veuillez suivre les étapes ci-dessous.

1. Sélectionnez « DynDNS.org » à partir du menu déroulant. Cliquez sur « Apply Changes [Enregistrer les Modifications] » .



2. Entrez votre nom d'utilisateur DynDNS dans le champ « User Name [nom d'utilisateur] » **(1)**.
3. Entrez votre mot de passe DynDNS.org dans le champ « Password » **(2)**.
4. Entrez votre nom de domaine DynDNS.org dans le champ « Domain Name » **(3)**.
5. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour mettre à jour l'adresse IP.

Lorsque votre FAI modifie l'adresse IP qui vous est attribuée, le Routeur s'occupe de la mise à jour des serveurs DynDNS.org, avec votre nouvelle adresse IP. Vous pouvez également le faire manuellement, en cliquant sur le bouton « Apply ChangesApply changes [Enregistrer les modifications] » **(4)**.

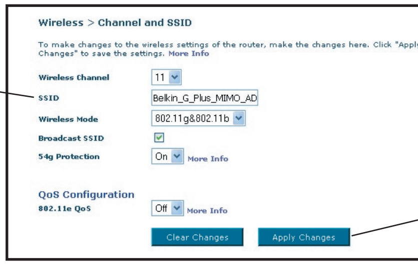


Sans Fil

L’onglet Sans Fil vous permet d’apporter des modifications aux paramètres de votre réseau sans fil. Vous pouvez apporter des modifications au nom du réseau sans fil (SSID), au canal d’opération et aux paramètres de chiffrement.

Canal et SSID

(1)



(2)

1. Modification du canal

Vous pouvez choisir parmi plusieurs canaux de fonctionnement. Aux États-Unis, il existe 11 canaux. Au Royaume-Uni et dans la plupart des pays d’Europe, il existe 13 canaux. Dans un petit nombre de pays, il existe d’autres exigences par rapport aux canaux. Votre Routeur est configuré de façon à fonctionner sur les canaux appropriés à votre pays de résidence. Le canal par défaut est le 11 (à moins que vous ne résidiez dans un pays où le canal 11 est interdit). Vous pouvez modifier le canal au besoin. S’il y a d’autres réseaux sans fil en fonction dans votre zone, votre réseau devrait fonctionner sur un canal différent de ceux utilisés par ces autres réseaux sans fil. Pour de meilleures performances, nous vous suggérons d’utiliser un canal éloigné des autres réseaux sans fil d’au moins cinq canaux. Par exemple, si un autre réseau fonctionne sur le canal 11, configurez votre réseau afin qu’il fonctionne sur le canal 6 ou moins. Pour modifier le canal, sélectionnez le canal à partir du menu déroulant. Cliquez sur « Apply Changes [Enregistrer les Modifications] » . Le changement est immédiat.

2. Modification du nom du réseau sans fil (SSID)

Le SSID (Service Set Identifier) correspond au nom de votre réseau sans fil. Le SSID par défaut du Routeur est « belkin54g ». Vous pouvez le modifier selon vos goûts, ou le laisser tel quel. S’il y a d’autres réseaux sans fil en fonction dans votre zone, assurez-vous que votre SSID est unique (n’est pas identique au SSID d’un autre réseau sans fil dans votre zone). Pour modifier le SSID, entrez le SSID désiré dans le champ SSID **(1)** et cliquez sur « Apply Changes [Enregistrer les informations] » pour valider le changement**(2)**. Le changement est immédiat. Si vous modifiez le SSID, vos ordinateurs sans fil doivent aussi être configurés à l’aide de ce même SSID afin qu’ils puissent se connecter à votre réseau sans fil. Reportez-vous à la documentation de votre adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

3. Utilisation de la fonction de diffusion ESSID

Pour des raisons de sécurité, vous pouvez choisir de ne pas diffuser le SSID de votre réseau. Ceci gardera le nom de votre réseau à l'abri des ordinateurs recherchant la présence de réseaux sans fil. Pour éteindre la fonction de diffusion du SSID, décochez la case à côté de l'option « Broadcast SSID [Diffusion du SSID] ». Le changement est immédiat. Chaque ordinateur doit maintenant être défini pour se connecter à votre SSID. Le paramètre « ANY » (TOUS) pour le SSID ne sera plus accepté. Reportez-vous à la documentation de votre adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

Remarque : Cette fonction avancée ne devrait être utilisée que par les utilisateurs expérimentés.

4. Utilisation de la fonction de commutation entre les modes sans fil

Votre Routeur est en mesure de fonctionner sous deux modes sans fil différents :

- **802.11b et 802.11g-** Choisissez cette option si votre réseau se composera de clients 802.11b et 802.11g.

- **802.11g -** Utilisez ce mode s'il n'y a pas de clients 802.11b dans votre réseau. Cette option vous permet de meilleures performances mais aucune connexion ne sera possible pour les clients 802.11b.

5. Switch en Mode Protégé

Faisant partie de la spécification du 802.11g, le mode Protégé assure un fonctionnement adéquat des clients et points d'accès 802.11g en présence d'un trafic 802.11b dense dans votre environnement réseau. Lorsque le mode Protégé est ACTIVÉ, le 802.11g balaye l'air pour détecter le trafic d'autres réseaux sans fil avant de transmettre les données. Ainsi, lorsque ce mode est utilisé dans un environnement avec un trafic 802.11b DENSE ou comportant des interférences, vous obtiendrez une meilleure performance. Si vous vous situez dans un environnement avec très peu, voire pas du tout, de trafic issu d'autres réseaux sans fil, vous obtiendrez une meilleure performance en désactivant le mode Protégé.

chiffrement/sécurité

Protection de votre réseau Wi-Fi

Voici quelques façons d'augmenter le niveau de protection de votre réseau sans fil et protéger vos données contre les intrusions. Cette section est destinée aux utilisateurs de réseaux sans fil à domicile, ou en entreprise (y compris les bureaux à domicile). Au moment de mettre ce manuel sous presse, quatre méthodes de chiffrement sont disponibles.

Nom	Wired Equivalent Privacy 64 bits	Wired Equivalent Privacy 128 bits	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acro-nyme	WEP 64 bits	WEP 128 bits	WPA-TKIP/AES (ou WPA)	WPA2-AES (ou WPA2)
Sécurité	Bon	Mieux	Meilleur	Meilleur
Caracté-ristiques	Clés fixes	Clés fixes	Chiffrement dynamique de la clé et authentification mutuelle	Chiffrement dynamique de la clé et authentifica-tion mutuelle
	Clés de chiffrement basées sur l'algorithme RC4 (clés de 40 bits)	Sécurité renforcée par rapport au WEP sur 64 bits, utilisant une clé de 104 bits, plus 24 bits additionnels pour des données générées par le système.	Le TKIP (temporal key integrity protocol) s'ajoute afin d'assurer la rotation des clés et de renforcer le chiffrement	L'AES (Advanced Encryption Standard) n'entraîne pas de perte de performances

WEP (Wired Equivalent Privacy)

Le WEP (Wired Equivalent Privacy) est un protocole courant qui renforce la sécurité de tous les dispositifs sans fil Wi-Fi. Le WEP est conçu dans le but d'offrir aux réseaux sans fil un niveau de protection comparable à celui des réseaux filaires.

WEP 64 bits

Le WEP 64 bits a été introduit la première fois avec un chiffrement de 64 bits, ce qui comprend une clé de 40 bits plus 24 bits supplémentaires composés de données générées par le système (64 bits au total). Certains fabricants se réfèrent au chiffrement sur 64 bits lorsqu'ils parlent du chiffrement sur 40 bits. Peu après le lancement de la technologie, les chercheurs ont découvert que le chiffrement sur 64 bits était trop simple à décoder.

WEP 128 bits

Pour contrer la faille de sécurité du WEP sur 64 bits, une méthode de chiffrement plus sécurisée, le WEP sur 128 bits, a été créée. Le WEP 128 bits comprend une clé de 104 bits plus 24 bits supplémentaires composés de données générées par le système (128 bits au total). Certains fabricants se réfèrent au chiffrement sur 128 bits lorsqu'ils parlent du chiffrement sur 104 bits.

La plupart des dispositifs sans fil disponibles sur le marché aujourd'hui prennent en charge le chiffrement WEP sur 64 et 128 bits, mais il se peut que vous possédiez un dispositif plus ancien ne prenant en charge que le WEP 64 bits. Tous les produits sans fil de Belkin prennent en charge le WEP 64 et 128 bits.

Clés de chiffrement

Après avoir choisi le mode de chiffrement (64 ou 128 bits), il est primordial de générer une clé de chiffrement. Si la clé de chiffrement n'est pas la même à travers tout le réseau sans fil, vos dispositifs sans fil ne seront pas en mesure de communiquer entre eux sur votre réseau.

Vous pouvez entrer votre clé en entrant la clé hexadécimale manuellement ou vous pouvez entrer une expression dans le champ « Passphrase [Expression] » et cliquer sur « Generate [Générer] » pour créer la clé. Une clé hexadécimale est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP 64 bits, vous devez entrer 10 caractères hexadécimaux. Pour le WEP 128 bits, vous devez entrer 26 caractères hexadécimaux.

L'expression mot de passe WEP n'est PAS la même chose que la clé WEP. Votre carte se sert de cette phrase de passe pour générer vos clés WEP, mais les différents fabricants peuvent avoir des méthodes différentes de générer ces clés. Si vous possédez des appareils venant de différents fabricants sur votre réseau, la solution la plus simple consiste à utiliser la clé hex WEP de votre Routeur ou de votre point d'accès et l'entrer manuellement dans la table de clés hex WEP, dans l'écran de configuration de votre adaptateur.

Utilisation d'une clé hexadécimale

Une clé hexadécimale est un mélange de chiffres et de lettres de A à F et de 0 à 9. Les clés 64 bits sont constituées par cinq nombres de deux chiffres. Les clés 128 bits comprennent 13 nombres à deux chiffres.

Par exemple :
AF 0F 4B C3 D4 = clé 64 bits
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé 128 bits
Dans les cases ci-dessous, créez vos clés en écrivant deux caractères de A à F et de 0 à 9. Vous utiliserez cette clé pour programmer les paramètres de chiffrement du Routeur et de vos ordinateurs sans fil.

Remarque aux utilisateurs de Mac : Les produits AirPort® d'Apple ne prennent en charge que le chiffrement sur 64 bits. Les produits Apple AirPort 2 prennent en charge le chiffrement sur 64 bits ou 128 bits. Veuillez vérifier la version de votre produit. Si vous ne parvenez pas à configurer le réseau avec le chiffrement sur 128 bits, essayez sur 64 bits.

WPA (Wi-Fi Protected Access)

Le WPA (Wi-Fi Protected Access) est une nouvelle norme Wi-Fi conçue afin d'apporter des améliorations aux caractéristiques de sécurité du WEP. Pour utiliser la sécurité WPA, vos dispositifs sans fil doivent être mis à jour avec les logiciels et les pilotes prenant en charge le WPA. Ces mises à jour peuvent être téléchargées à partir du site Web de leurs fabricants respectifs. Il existe deux types de sécurité par WPA : WPA-Personal (PSK) et WPA-Enterprise (RADIUS).

WPA-Personal (PSK)

Le WPA-PSK utilise ce qu'on appelle une clé pré-partagée comme clé de sécurité. Une clé réseau est en quelque sorte un mot de passe composé de 8 à 63 caractères. Il peut être composé de lettres, de chiffres ou de symboles. Chaque client utilise la même clé réseau pour accéder au réseau. De façon générale, ce mode est utilisé pour les réseaux domestiques.

WPA-Enterprise (RADIUS)

Avec ce système, un serveur radius distribue les clés réseau aux clients de façon automatique. Ce système se retrouve surtout en entreprise. Pour la liste des produits Belkin prenant en charge le WPA, visitez notre site Web au **www.belkin.com/networking**.

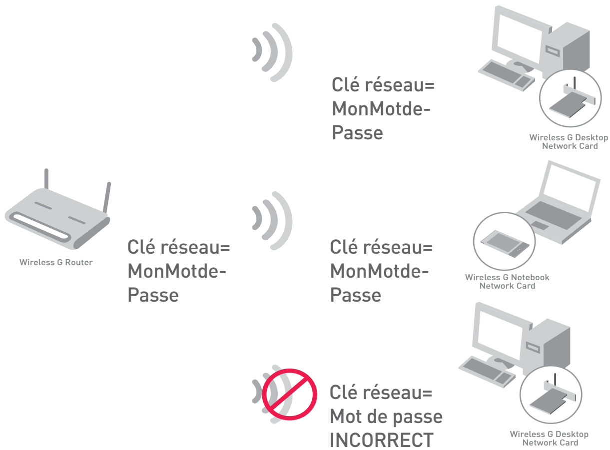
WPA2 (WiFi Protected Access)

Le WPA2 est la deuxième génération de chiffrement WPA, basé sur la norme 802.11i. Elle offre un niveau de protection sans fil plus élevé en combinant une authentification réseau avancée et une méthode de chiffrement AES renforcée. Tout comme la sécurité WPA, le WPA2 est disponible en mode WPA2-Personal (PSK) et en mode WPA2-Enterprise (RADIUS). De façon générale, le WPA2-Personal (PSK) se retrouve dans le cas d'un réseau domestique, alors que le WPA2-Enterprise (RADIUS) se retrouve en environnement d'enreprise, où un serveur radius externe distribue la clé réseau aux clients de façon automatique.

Partage des clés réseau

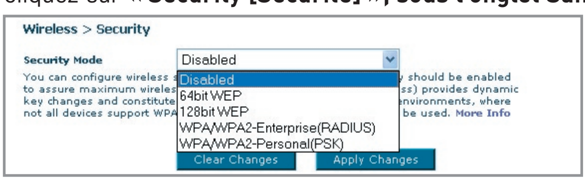
La plupart des dispositifs Wi-Fi désactivent la fonction de sécurité par défaut. Après avoir mis en route votre réseau, vous devez activer le WEP ou le WPA/WPA2 et vous assurer que tous les dispositifs sans fil de votre réseau partagent la même clé réseau.

La Carte Réseau Sans Fil G+ MIMO pour ordinateur de bureau ne peut pas accéder au réseau parce qu'il utilise une clé réseau différente que celle configurée sur votre Routeur Sans Fil G+ MIMO.



Modification des paramètres de sécurité sans fil

Votre Routeur comprend la toute dernière norme de sécurité, appelée WPA/WPA2 (Wi-Fi Protected Access). En outre, il prend en charge les normes de sécurité plus anciennes telles que le WEP (Wired Equivalent Privacy). Par défaut, la sécurité sans fil est désactivée. Pour activer la sécurité, vous devez d'abord déterminer la méthode de chiffrement de votre choix. Pour accéder aux paramètres de sécurité, cliquez sur **« Security [Sécurité] », sous l'onglet Sans Fil.**



Configuration du WEP

Chiffrement WEP 64 bits

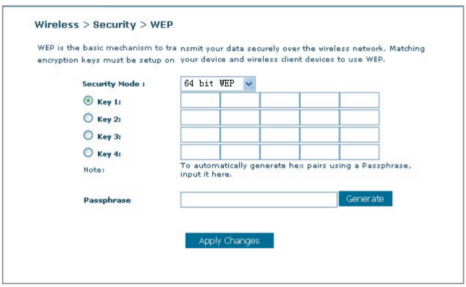
1. Sélectionnez « WEP 64 bits » dans le menu déroulant.

2. Après avoir sélectionné votre mode de chiffrement WEP, entrez votre clé hexadécimale manuellement.

Une clé hexadécimale est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP 64 bits, vous devez entrer 10 caractères hexadécimaux.

Par exemple :

AF 0F 4B C3 D4 = clé WEP 64 bits



3. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Le chiffrement de votre Routeur est maintenant configuré. Chaque ordinateur de votre réseau sans fil devra maintenant être configuré avec les mêmes paramètres de sécurité.

AVERTISSEMENT : Si vous configurez le Routeur Sans Fil ou le Point d'Accès à partir d'un ordinateur doté d'un client sans fil, vous perdez votre connexion jusqu'à ce que vous ayez activé la sécurité sur votre client sans fil. N'oubliez pas de noter votre clé avant d'enregistrer les modifications.

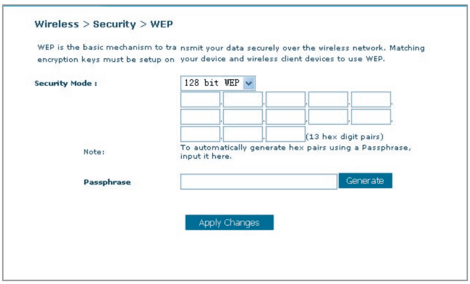
Chiffrement WEP 128 bits

1. Sélectionnez « WEP 128 bits » dans le menu déroulant.
2. Après avoir sélectionné votre mode de chiffrement WEP, entrez votre clé hexadécimale manuellement.

   Une clé hexadécimale est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP 128 bits, vous devez entrer 26 caractères hexadécimaux.

   Par exemple :

   C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé WEP 128 bits



3. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Le chiffrement de votre Routeur est maintenant configuré. Chaque ordinateur de votre réseau sans fil devra maintenant être configuré avec les mêmes paramètres de sécurité.

AVERTISSEMENT : Si vous configurez le Routeur Sans Fil ou le Point d'Accès à partir d'un ordinateur doté d'un client sans fil, vous perdez votre connexion jusqu'à ce que vous ayez activé la sécurité sur votre client sans fil. N'oubliez pas de noter votre clé avant d'enregistrer les modifications.

Configuration du WPA

Remarque : Pour utiliser la sécurité par WPA, votre client doit être mis à jour avec les logiciels et les pilotes qui le prennent en charge. Au moment de mettre ce manuel sous presse, une rustine de sécurité est disponible pour téléchargement gratuit, auprès de Microsoft. Cette rustine ne fonctionne qu'avec Windows XP. Vous devrez en outre télécharger le

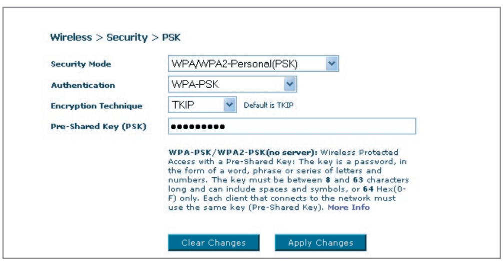
plus récent pilote pour votre Carte Réseau Sans Fil G pour ordinateur de bureau ou portable de Belkin, que vous trouverez sur le site de l’assistance technique de Belkin. Les autres systèmes d’exploitation ne sont pas pris en charge pour le moment. La rustine de Microsoft ne prend en charge que les dispositifs avec pilotes compatibles WPA, tels que les produits 802.11g de Belkin.

Il existe deux types de sécurité par WPA : WPA-Personal (PSK) et WPA-Enterprise (RADIUS). Le WPA-Personal (PSK) utilise ce qu’on appelle une clé pré-partagée en tant que clé de sécurité. Une clé pré-partagée est en quelque sorte un mot de passe composé de 8 à 63 caractères. Il peut être composé de lettres, de chiffres ou de symboles. Chaque client utilise la même clé pour accéder au réseau. De façon générale, ce mode est utilisé pour les réseaux domestiques.

Le WPA-Enterprise (RADIUS)consiste en un système où le serveur radius distribue automatiquement les clés aux clients. Ce système se retrouve surtout en entreprise.

Configuration WPA-Personal (PSK)

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA/WPA2-PSK ».
2. Sélectionnez « “WPA-PSK » pour l’authentification.
3. À « Encryption Technique [Technique de chiffrement] », choisissez « TKIP ». Ce paramètre devra être identique à celui des clients que vous configurerez.
4. Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres ou symboles). Cette clé doit être utilisée pour tous les clients branchés au réseau. Par exemple, votre clé pré-partagée peut ressembler à : « Clé réseau de la famille Dupont ».



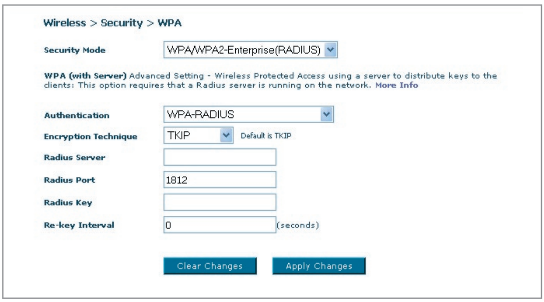
5. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Configuration des paramètres WPA-Enterprise (RADIUS)

Si votre réseau utilise un serveur Radius pour distribuer les clés aux clients, veuillez utiliser ce paramètre.

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA/WPA2—Enterprise (RADIUS) ».

2. Sélectionnez « WPA-RADIUS » pour l'authentification.
3. À « Encryption Technique [Technique de chiffrement] », choisissez « TKIP ». Ce paramètre devra être identique à celui des clients que vous configurerez.
4. Entrez l'adresse IP de votre serveur Radius dans le champ « Radius server [Serveur Radius] ».
5. Entrez la clé Radius dans le champ « Clé Radius ».
6. Entrez l'intervalle de clé. L'intervalle de clé correspond au nombre de fois où les clés sont distribuées (en paquets).
7. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.



Configuration requise pour le WPA2

IMPORTANT : Pour utiliser la sécurité WPA2, tous vos ordinateurs et vos adaptateurs clients sans fil doivent être mis à niveau avec des rustines, des clients et des logiciels utilitaires clients prenant en charge le WPA2. Au moment de mettre ce manuel sous presse, plusieurs rustines de sécurité sont disponibles pour téléchargement gratuit, auprès de Microsoft. Ces patchs ne fonctionnent qu'avec Windows XP. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment.

Pour les ordinateurs sous Windows XP sans Service Pack 2 (SP2), un fichier Microsoft appelé « Windows XP Support Patch for Wireless Protected Access (KB 826942) » est disponible pour téléchargement gratuit à http://support.microsoft.com/?kbid=826942.

Pour Windows XP avec Service Pack 2, Microsoft a lancé un fichier pour téléchargement gratuit afin de mettre à niveau les composants du client sans fil pour prise en charge du WPA2 (KB893357). Vous pouvez télécharger la mise à jour ici : http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

IMPORTANT : Vous devez également vous assurer que toutes vos cartes/adaptateurs clients sans fil prennent en charge le WPA2, et que vous avez téléchargé et installé le pilote le plus récent. Un pilote mis à jour pour la plupart des cartes sans fil Belkin est disponible pour téléchargement à partir du site de l'assistance technique Belkin : www.belkin.com/networking.

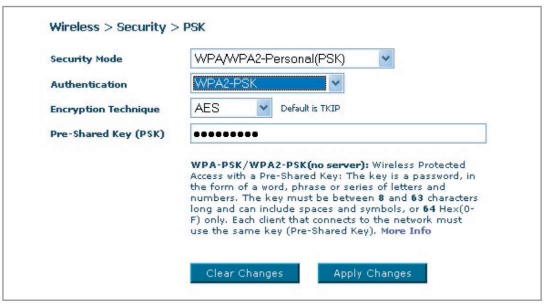
Configuration WPA2-Personal (PSK)

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA/WPA2-PSK (PSK) ».

2. Sélectionnez « WPA2-Personal (PSK) » pour l'authentification.

3. À « Encryption Technique [Technique de chiffrement] », choisissez « AES ». Ce paramètre devra être identique à celui des clients que vous configurerez.

4. Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres ou symboles). Cette clé doit être utilisée pour tous les clients branchés au réseau. Par exemple, votre clé pré-partagée peut ressembler à : « Clé réseau de la famille Dupont ».



5. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Configuration des paramètres WPAw-Enterprise (RADIUS)

Si votre réseau utilise un serveur Radius pour distribuer les clés aux clients,

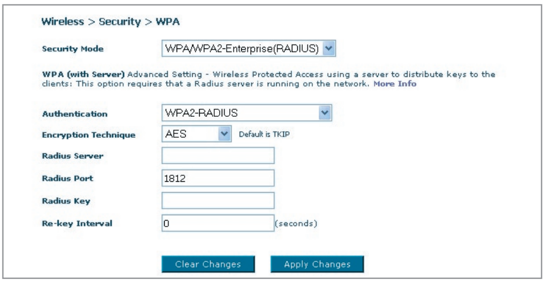
veuillez utiliser ce paramètre.

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA/WPA2—Enterprise (RADIUS) ».

2. Sélectionnez « WPA-RADIUS » pour l'authentification.

3. À « Encryption Technique [Technique de chiffrement] », choisissez « AES ». Ce paramètre devra être identique à celui des clients que vous configurerez.

4. Entrez l'adresse IP de votre serveur Radius dans le champ « Radius server [Serveur Radius] ».
5. Entrez la clé Radius dans le champ « Clé Radius ».
6. Entrez l'intervalle de clé. L'intervalle de clé correspond au nombre de fois où les clés sont distribuées (en paquets).
7. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.



IMPORTANT : Assurez-vous que vos ordinateurs sans fil sont mis à jour afin de prendre en charge le WPA2 et possèdent les réglages appropriés permettant une connexion au Routeur.

Configuration de votre adaptateur réseau pour utilisation de la fonction de sécurité

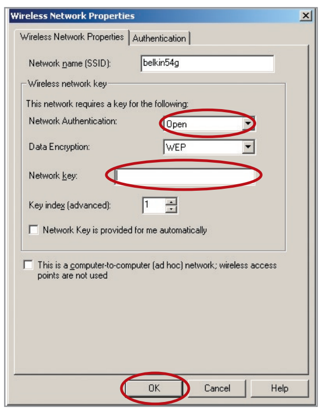
Remarque : Cette section vous informe sur la configuration de votrea daptateur réseau pour utilisation de la fonction de sécurité. Jusqu'à maintenant, vous avez configuré votre Routeur ou Point d'Accès Sans Fil afin qu'il(s) utilise(nt) le WPA, le WPA2 ou le WEP. Pour obtenir une connexion sans fil, tous les cartes/adaptateurs réseau sans fil doivent maintenant être configurés avec ces mêmes paramètres de sécurité.

Les Cartes Réseau Belkin G+ MIMO sont dotées d'un utilitaire réseau simple d'utilisation. Cliquez sur le nom du réseau sans fil (SSID) dans la liste des réseaux disponibles et entrez votre clé pré-partagée (PSK). Pour en savoir plus, consultez le manuel de l'utilisateur de votre carte réseau Belkin.

La plupart des ordinateurs peuvent également être configurés à l'aide de l'écran Propriétés réseau sans fil du Routeur, faisant partie intégrante du système d'exploitation Windows. Voici deux exemples :

Connexion de votre ordinateur à un réseau sans fil utilisant une clé WEP 64 ou 128 bits :

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte sans fil.
2. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Configure [Configurer] ».
3. Sous « Data Encryption [Chiffrement de données] », sélectionnez « WEP ».
4. Assurez-vous que la case « The key is provided for me automatically [J'obtiens une clé automatiquement] » n'est pas cochée. Si vous utilisez cet ordinateur pour vous connecter à un réseau d'entreprise, prenez conseil auprès de votre administrateur réseau afin de savoir si cette case doit être cochée.
5. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

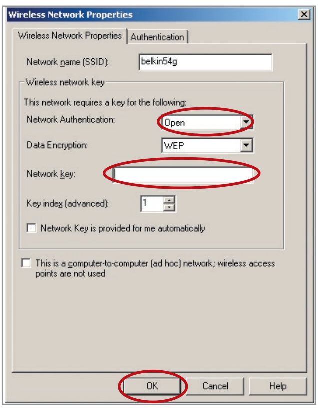


Important : Une clé WEP est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP sur 128 bits, vous devez entrer 26 caractères hexadécimaux. Pour le WEP sur 64 bits, vous devez entrer 10 caractères hexadécimaux. Cette clé réseau doit être identique à la clé que vous avez assignée à votre Routeur ou Point d'Accès Sans Fil.

6. Cliquez « OK » pour enregistrer les paramètres.

Connexion de votre ordinateur à un réseau sans fil utilisant le WPA-PSK (sans serveur)

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte sans fil.
2. Sous l'onglet « Wireless Network [Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Configure [Configurer] ».
3. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA-PSK (No server) [WPA-PSK (Sans serveur)] ».
4. Entrez votre clé WPA dans la boîte « Network Key [Clé Réseau] ».

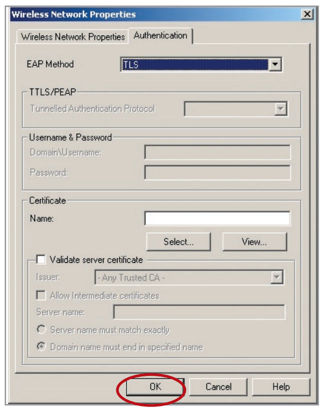


Important : Une clé WPA-PSK est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WPA-PSK, vous devez entrer de 8 à 63 caractères. Cette clé réseau doit être identique à la clé que vous avez assignée à votre Routeur ou Point d'Accès Sans Fil.

5. Cliquez « OK » pour enregistrer les paramètres.

Connexion de votre ordinateur à un réseau sans fil utilisant le WPA (avec serveur radius)

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte sans fil.
2. Sous l'onglet « Wireless Network [Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Configure [Configurer] ».
3. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA ».
4. Sous l'onglet « Authentication [Authentification] », choisissez les paramètres spécifiés par l'administrateur de votre réseau.
5. Cliquez « OK » pour enregistrer les paramètres.



Configuration du WPA/WPA2 pour cartes réseau sans fil pour ordinateurs de bureau ou portable (autres que Belkin)

Pour les Cartes réseau sans fil pour ordinateurs de bureau ou portable ne prenant pas en charge le WPA, une rustine de Microsoft, nommée « Windows XP Support Patch for Wireless Protected Access » est disponible pour téléchargement gratuit.

Prenez note : Cette rustine ne fonctionne qu'avec Windows XP. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment.

Important : Vous devrez en outre vous assurer que le fabricant de votre carte sans fil prend en charge le WPA/WP2 et que vous avez téléchargé et installé le pilote le plus récent, que vous trouverez sur leur site web.

Systèmes d'exploitation pris en charge :

- **Windows XP Professionnel**
- **Windows XP Édition Familiale**

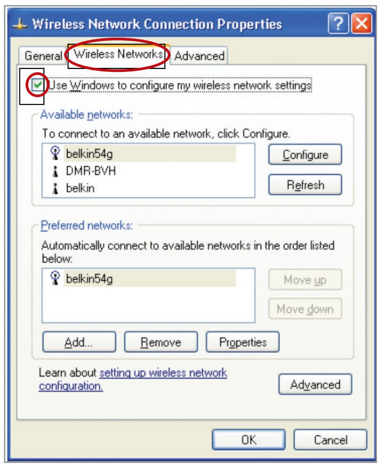
Configuration de l'Utilitaire Réseau Sans Fil de Windows XP pour utilisation du WPA/WPA2-PSK

Afin d'utiliser le WPA-PSK, assurez-vous d'utiliser l'Utilitaire Réseau Sans Fil de Windows. Procédez comme suit :

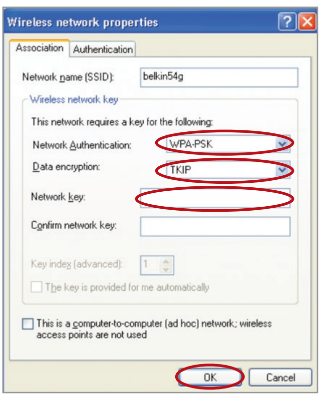
1. Sous Windows XP, cliquez Démarrer > Panneau de Configuration > Connexions Réseaux et Internet.

2. Cliquez avec le bouton droit de la souris sur « Wireless Network Connection [Connexion Réseau Sans Fil] » et sélectionnez « Properties [Propriétés] ».

3. En cliquant avec le bouton droit de votre souris sur « Wireless Networks [Réseaux Sans Fil] », vous verrez une fenêtre s'afficher comme suit : Assurez-vous que la boîte « Use Windows to configure my wireless network settings [Utiliser Windows pour configurer mes paramètres réseau sans fil] » est cochée.



4. Sous l'onglet « Wireless Networks [Réseaux Sans Fil] », cliquez sur le bouton « Configure [Configurer] » et vous verrez une fenêtre s'afficher comme suit :



5. Pour l'utilisateur de réseau domestique ou de petite entreprise, sélectionnez « WPA-PSK » ou « WPA2-PSK » sous « Network Authentication [Authentification Réseau] ».

Remarque : Sélectionnez le WPA si vous utilisez cet ordinateur pour vous brancher à un réseau d'entreprise, qui à son tour prend en charge un serveur d'authentification tel que le serveur RADIUS. Renseignez-vous auprès de l'administrateur de votre réseau pour de plus amples informations.

6. Sélectionnez « TKIP » ou « AES » sous « Data Encryption [Chiffrement de données] ». Ce paramètre devra être identique à ce lui que vous configurerez sur le Routeur.

7. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

Important : Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres ou symboles). Cette clé doit être utilisée pour tous les clients branchés au réseau.

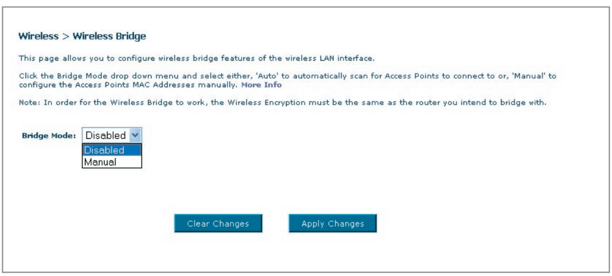
8. Cliquez « OK » pour enregistrer les paramètres.

Pont Sans Fil

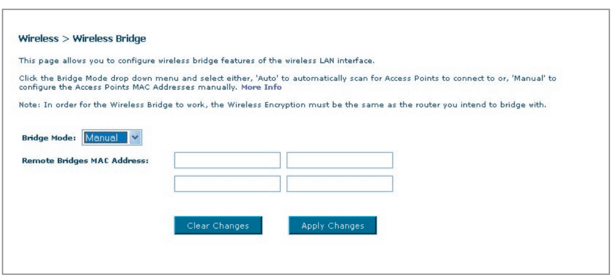
Le pont sans fil ou système de distribution sans fil (Wireless Distribution System - WDS) est utilisé pour connecter des routeurs et des points d'accès sans fil dans le but d'étendre la portée d'un réseau.

Cliquez sur le menu déroulant en regard de « Bridge Mode [Mode de Pontage] » et choisissez parmi :

Désactivé :Désactiver le pontage sans fil (défaut)



Manuel : Entrez manuellement une ou des adresse(s) MAC de points d'accès afin d'établir une passerelle.



1 Les canaux sans fil doivent être identiques sur le Routeur et le Point d'accès.

2 Les paramètres de sécurité (WEP) doivent être identiques sur le Routeur et le Point d'accès.

3 Si le filtrage MAC est activé, assurez-vous d'ajouter la ou les adresse(s) MAC WLAN du Routeur/Point d'accès afin de permettre à ceux-ci de communiquer.

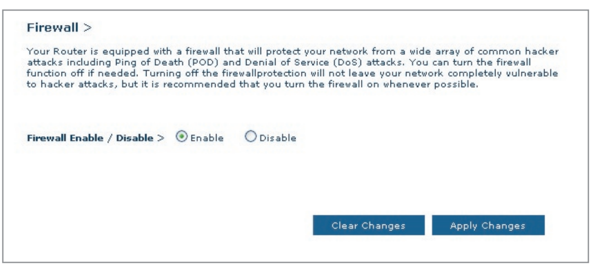
4 Si vous utilisez un réseau protégé par WPA, le SSID des deux Points d'accès doivent être identique.

Pare-feu

Votre Routeur est équipé d'un pare-feu qui sert à protéger le réseau d'une variété d'attaques de pirates informatiques, y compris :

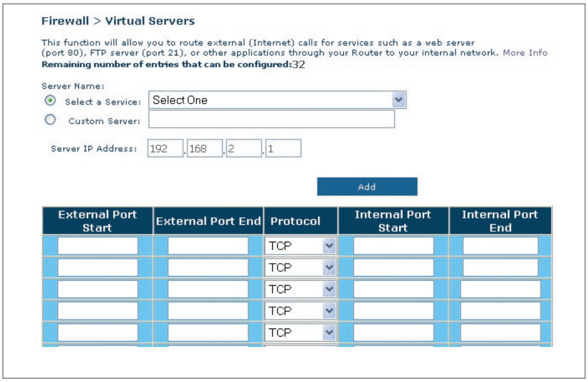
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

Le pare-feu masque en outre les ports réseau qui font fréquemment l'objet d'attaques. Ces ports sont invisibles, ce qui veut dire qu'ils n'existent pas pour un potentiel hacker. Vous pouvez désactiver la fonction de pare-feu au besoin. Toutefois, il est recommandé de que le pare-feu soit activé en tout temps. Désactiver le pare-feu ne rendra pas votre réseau totalement vulnérable aux attaques provenant des pirates informatiques, mais il est recommandé d'activer le pare-feu en tout temps.



Serveurs Virtuels

Les serveurs virtuels vous permettent d'acheminer, via le Routeur et vers votre réseau interne, les appels externes (Internet) de services tels qu'un serveur web (port 80), un serveur FTP (port 21) ou d'autres applications. Parce que vos ordinateurs internes sont protégés par le pare-feu, les machines provenant de l'Internet ne peuvent accédez à ceux-ci puisqu'ils sont invisibles . Si vous devez configurer la fonction de Serveur Virtuel pour une application particulière, vous devez contacter le fabricant de votre application et déterminer quels paramètres de ports sont nécessaires. Vous pouvez entrer l'information à propos des ports manuellement dans le Routeur.



Choix d'une application

Vous pouvez choisir vos applications à partir d'une liste d'applications courantes. Cliquez sur « Select a service [Choisir un service] » puis choisissez l'application dans la liste déroulante. Les paramètres seront transférés à la première rangée disponible. Cliquez sur « Add [Ajouter] » pour sauvegarder les paramètres de cette application.

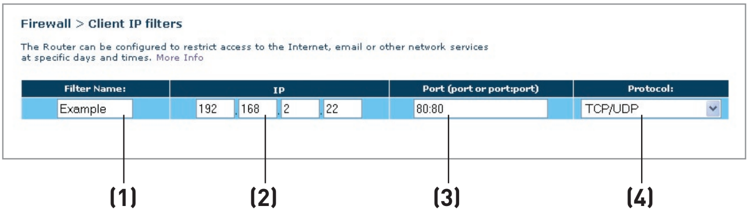
Saisie manuelle des paramètres du serveur virtuel

Pour entrer les paramètres manuellement, cliquez sur « Custom Server [Serveur personnalisé] » et entrez un nom pour ce serveur. Entrez l'adresse IP du serveur dans l'espace fourni, pour la machine internet et le(s) port(s) à franchir. Choisissez le type de protocole (TCP ou UDP) et cliquez sur « Add [Ajouter] ».

L'ouverture des ports de votre pare-feu peut compromettre la sécurité de votre réseau. Vous pouvez rapidement activer ou désactiver cette fonction. Il est recommandé de désactiver cette fonction lorsque vous n'utilisez pas d'application spécifique.

Filtres d'IP des clients

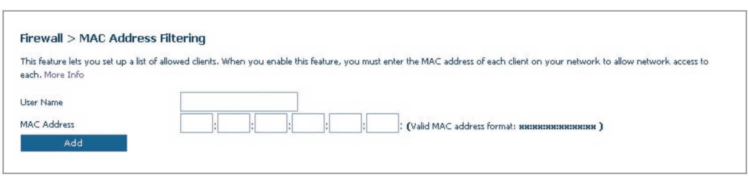
Le Routeur peut être configuré de sorte à limiter l'accès de certains ordinateurs à Internet, au courrier électronique et autres fonctions réseaux, à des jours et des heures donnés.



Pour restreindre l'accès à un seul ordinateur, par exemple, entrez le nom du filtre dans le champ « Filter Name [Nom du filtre] » **(1)** et l'adresse IP de l'ordinateur à qui vous désirez restreindre l'accès dans le champ de l'adresse IP **(2)**. Ensuite, entrez « 80 » et « 80 » dans les champs « Port » **(3)**. Sélectionnez le protocole à partir du menu déroulant « Protocol [Protocole] » **(4)** Cliquez sur « Apply Changes [Enregistrer les Modifications] » . L'ordinateur à l'adresse IP que vous avez spécifiée ne pourra dorénavant plus accéder à l'Internet.

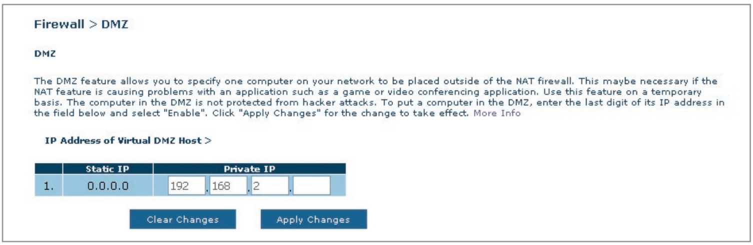
Filtrage des adresses MAC

Le filtrage d'adresses MAC est une fonction de sécurité puissante qui vous permet de spécifier les ordinateurs autorisés à se connecter au réseau. Tout ordinateur non spécifié dans les paramètres du filtre et qui tente d'accéder au réseau se verra refuser l'accès. Lorsque vous activez cette fonction, vous devez entrer un nom pour l'utilisateur et l'adresse MAC de chaque client de votre réseau, pour permettre à chacun d'accéder au réseau. Ensuite, cliquez sur « Add [Ajouter] » pour enregistrer les paramètres.



DMZ (zone démilitarisée)

Si un de vos PC clients ne peut éxécuter une application Internet convenablement parce qu'il se trouve derrière un pare-feu, vous pouvez modifier les restrictions en permettant l'accès à internet bidirectionnel. Cette opération peut s'avérer nécessaire si la traduction d'adresse réseau (NAT) empêche le bon fonctionnement d'applications telles que les jeux ou les vidéoconférences. Servez-vous de cette fonction au besoin. **L'ordinateur placé dans la zone DMZ ne sera pas protégé contre les attaques provenant de hackers.**

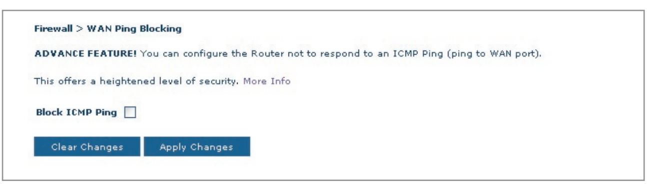


Pour placer un ordinateur dans la zone DMZ, entrez son adresse IP de réseau local dans le champ de saisie d'IP privée, et cliquez sur « Apply Changes [Enregistrer les Modifications] » pour que celles-ci soient prises en compte.

Blocage du ping ICMP

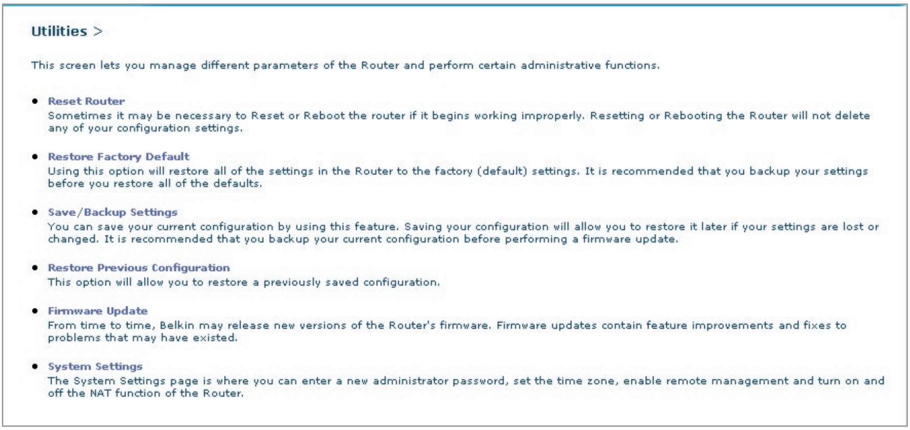
Les pirates informatiques utilisent une technique appelée Pinging pour dénicher sur Internet leurs victimes potentielles. En faisant un ping vers une adresse IP particulière et en recevant une réponse de la part de celle-ci, un pirate informatique peut décider de s'intéresser à ce qui se trouve derrière cette adresse. Le Routeur peut être défini de façon à ne pas répondre à un ping ICMP provenant de l'extérieur. Ceci rehausse le niveau de sécurité de votre Routeur.

Pour désactiver la réponse au ping, sélectionnez « Block ICMP Ping [Bloquer le ping ICMP] » **(1)**, puis cliquez sur « Apply Changes [Enregistrer les modifications] ». Le Routeur ne répondra pas aux pings ICMP.



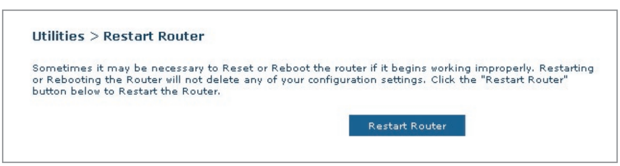
Utilitaires

L'écran Utilitaires vous permet de gérer plusieurs paramètres du Routeur et accomplir certaines tâches administratives.



Redémarrer le Routeur

Il peut parfois être utile de redémarrer le Routeur lorsque celui-ci fonctionne de façon incongrue. Le redémarrage ou le réamorçage du Routeur ne supprimera AUCUN de vos paramètres de configuration.



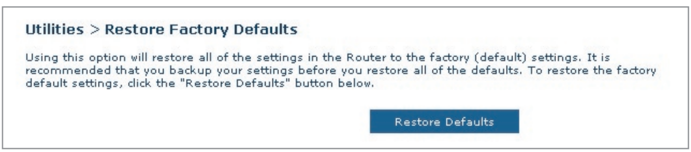
Redémarrer le Routeur pour rétablir le fonctionnement normal

1. Cliquez sur le bouton « Restart Router [Redémarrer le Routeur] ».
2. Le message suivant apparaît. Cliquez sur « OK » pour redémarrer le Routeur.

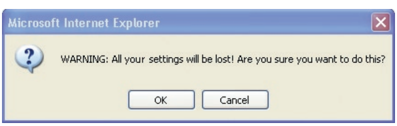


Rétablir les Paramètres par Défaut du Constructeur

Cette option rétablira les paramètres du Routeur vers les paramètres par défaut du fabricant. Nous vous recommandons de faire une copie de sauvegarde de vos paramètres avant de rétablir la configuration par défaut.

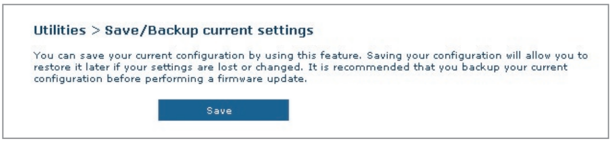


1. Cliquez sur le bouton « Restore Defaults [Rétablir les Paramètres] ».
2. Le message suivant apparaît. Cliquez sur « OK » pour rétablir les paramètres par défaut du fabricant.

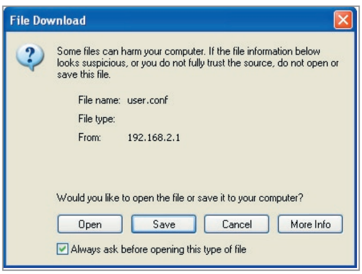


Enregistrer/Sauvegarder les paramètres actuels

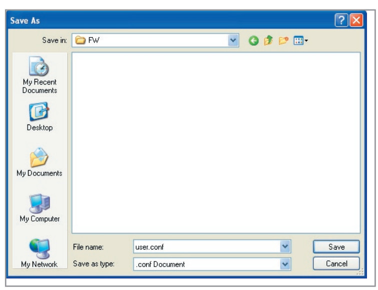
Vous pouvez sauvegarder votre configuration actuelle grâce à cette fonction. Cela vous permettra de la rétablir plus tard si vous perdez les paramètres ou s'ils sont modifiés. Nous vous recommandons de faire une copie de vos paramètres avant de mettre à jour le micrologiciel.



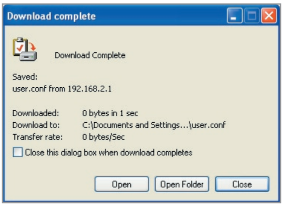
1. Cliquez « Save [Enregistrer] ». La fenêtre « File Download [Téléchargement de fichier] » apparaît. Cliquez sur « Save [Enregistrer] ».



2. Une nouvelle fenêtre s'ouvrira pour vous permettre de choisir l'endroit où se trouve le fichier de configuration. Sélectionnez un emplacement. Vous pouvez donner n'importe quel nom à votre fichier, mais assurez-vous de pouvoir le retrouver plus tard. Lorsque vous avez choisi l'emplacement et le nom du fichier, cliquez sur « Save [Enregistrer] ».



3. Lorsque la sauvegarde est terminée, vous verrez la fenêtre ci-dessous. Cliquez sur « Close [Fermer] ».

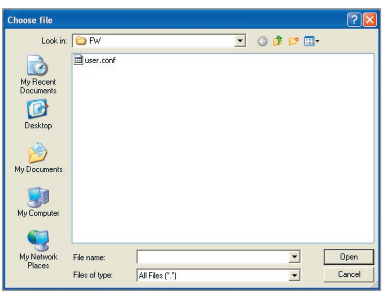


Votre configuration est maintenant sauvegardée.

Rétablir les Paramètres Précédents

Cette option vous permet de rétablir une configuration sauvegardée préalablement.

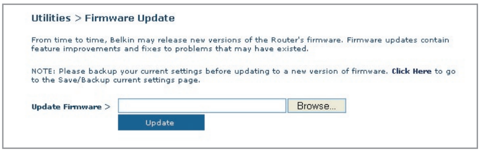
1. Cliquez « Browse [Parcourir] ». Une nouvelle fenêtre s'ouvrira pour vous permettre de choisir l'endroit où se trouve le fichier de configuration. Tous les fichiers de configuration se terminent par l'extension « .conf ». Localisez le fichier de configuration désiré et double-cliquez sur celui-ci.



2. Cliquez sur « Open [Ouvrir] ».

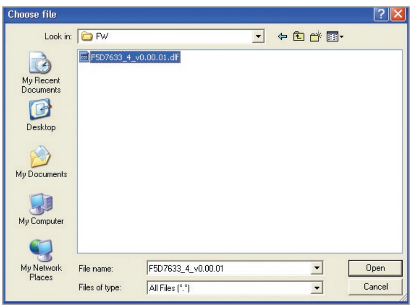
Mise à jour du micrologiciel

De temps à autre, Belkin peut lancer une nouvelle version du micrologiciel du Routeur. Ces mises à jour peuvent contenir des améliorations et des solutions aux problèmes existants. Lorsque Belkin lance un nouveau micrologiciel, vous pouvez le télécharger à partir du site de mises à jours de Belkin, et mettre à jour votre micrologiciel avec la toute dernière version.



Mise à jour du micrologiciel du Routeur

1. À la page de mise à jour du micrologiciel, cliquez sur « Browse [Parcourir] ». Une nouvelle fenêtre s'ouvrira pour vous permettre de choisir l'endroit où se
trouve le fichier de mise à jour du micrologiciel.



2. Parcourez afin de localiser le fichier que vous venez de télécharger. Sélectionnez le fichier en double-cliquant sur le nom du fichier.

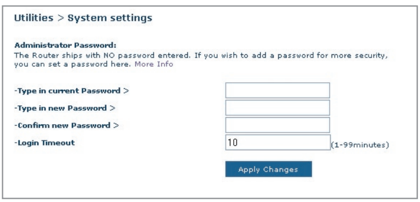
3. Cliquez sur « Update [Mettre à jour] » afin de mettre à jour le micrologiciel avec la nouvelle version.

Paramètres du Système

À la page des Paramètres du Système, vous pouvez entrer un nouveau mot de passe administrateur, régler le fuseau horaire, activer la gestion à distance, et activer/désactiver la fonction de NAT du Routeur.

Entrer ou modifier le mot de passe administrateur

Le Routeur est livré SANS mot de passe défini. Si par souci de sécurité vous désirer ajouter un mot de passe, vous pouvez le configurer ici. Écrivez votre mot de passe et conservez-le dans un endroit sûr, puisque vous en aurez besoin plus tard pour vous connecter au Routeur. Nous recommandons aussi l'ajout d'un mot de passe si vous prévoyez utiliser la fonction de gestion à distance du Routeur.



Modification du délai de temporisation de la connexion

L'option de temporisation de la connexion vous permet de déterminer une plage horaire pendant laquelle vous pouvez être connecté à l'interface de configuration avancée du Routeur. La temporisation débute lorsqu'il n'y a plus d'activité. Par exemple, vous avez apporté des modifications au niveau de l'interface de configuration évoluée, puis vous avez quitté l'ordinateur sans cliquer sur « Logout [Déconnexion] ». En prenant pour exemple un temporisateur paramétré à 10 minutes, votre connexion prendra fin 10 minutes après votre départ. Vous devrez donc vous connecter à nouveau au Routeur pour apporter d'autres modifications. L'option de temporisation de la connexion sert à des fins de sécurité, et le paramètre par défaut est 10 minutes.

Remarque : Un seul ordinateur à la fois peut être connecté à l'interface de configuration avancée du Routeur.

Définition d'un fuseau horaire

Le Routeur harmonise le temps en se connectant à un serveur SNTP (Simple Network Time Protocol). Ceci lui permet de synchroniser l'horloge du système avec l'Internet planétaire. L'horloge ainsi synchronisée est utilisée par le routeur pour garder un journal de connexions et pour contrôler le filtrage des clients.

Sélectionnez le serveur temporel NTP et votre fuseau horaire, puis cliquez sur « Apply Changes [Enregistrer les modifications] ». L'horloge du système peut ne pas être mise à jour immédiatement. Laissez au minimum 15 minutes au Routeur pour contacter les serveurs horaires sur Internet et obtenir une réponse. Vous ne pouvez pas modifier l'horloge vous-même.



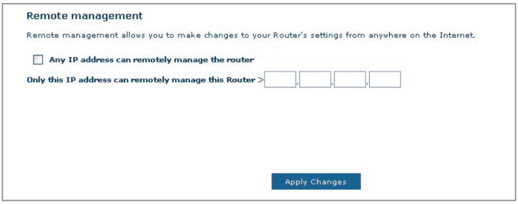
Activer la gestion à distance

Avant d'activer cette fonctionnalité évoluée de votre Routeur Belkin, **ASSUREZ-VOUS D'AVOIR DÉFINI VOTRE MOT DE PASSE ADMINISTRATEUR**. La gestion à distance vous permet d'apporter des changements aux paramètres de votre Routeur, où que vous soyez grâce à l'Internet.
Cliquez sur le bouton « Change Settings [Modifier les paramètres] » pour faire apparaître la page « Remote Management [Gestion à distance] ».

Il existe deux méthodes de gestion à distance du Routeur. La première consiste à accéder au Routeur depuis un endroit quelconque d'Internet en sélectionnant « Any IP address can remotely manage the Router [Toute adresse IP peut gérer le Routeur à distance] ». Lorsque vous aurez entré votre adresse IP WAN depuis un ordinateur sur Internet, un écran de connexion apparaîtra. Vous devrez y entrer le mot de passe du Routeur.

La seconde méthode consiste à autoriser une seule adresse IP spécifique à gérer le Routeur à distance. Cette méthode est la plus sécuritaire, mais la moins pratique. Pour y avoir recours, entrez l'adresse IP autorisée à accéder au Routeur dans le champ fourni à cet effet, puis sélectionnez « Only this IP address can remotely manage the Router [Seule cette adresse IP est autorisée à gérer le Routeur à distance] ». Avant d'activer cette fonction, il est FORTEMENT RECOMMANDÉ d'entrer un mot de passe administrateur. Si vous laissez le mot de passe vide, vous autorisez potentiellement des intrusions sur le Routeur.

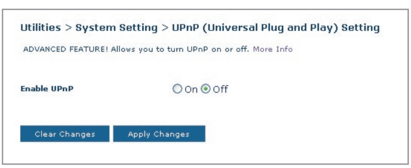
Cliquez sur le bouton « Apply Changes [Enregistrer les modifications] » pour enregistrer les paramètres.



Activer/Désactiver l'UPnP

L'UPnP (Universal Plug-and-Play) est une fonction avancée unique à votre Routeur. C'est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux, et d'autres applications compatibles avec l'UPnP. Certaines applications nécessitent que le pare-feu du Routeur soit configuré selon certains paramètres pour fonctionner adéquatement. Pour ce faire, vous devez habituellement ouvrir des ports TCP et UDP, et parfois même configurer des ports de déclenchement. Une application qui est compatible avec l'UPnP possède la capacité de communiquer avec le Routeur, lui indiquant la façon dont le pare-feu doit être configuré. Le routeur est livré avec la fonction UPnP désactivée. Si vous utilisez une application qui est compatible avec l'UPnP, et si vous désirez bénéficier des avantages de l'UPnP, vous pouvez activer la fonction UPnP.

Cliquez sur le bouton « Change Settings [Modifier les paramètres] » pour faire apparaître la page « UPnP Setting [Paramètre UPnP] ». Sélectionnez ensuite « On [Activé] » à « Enable UPnP [Activer l'UPnP] ». Cliquez sur le bouton « Apply Changes [Enregistrer les modifications] » pour enregistrer les paramètres.



Problème :

Le témoin ADSL est éteint.

Solution :

1. Vérifiez la connexion entre le Routeur et la ligne ADSL. Assurez-vous que le câble réseau provenant de la ligne ADSL est branché au port « ADSL » du Routeur.
2. Assurez-vous que le courant arrive au Routeur. Le témoin d'alimentation ⏻ à l'avant du Routeur doit être allumé.

Problème :

Le témoin Internet est éteint.

Solution :

1. Assurez-vous que le câble réseau provenant de la ligne ADSL est branché au port « ADSL » du Routeur ☎ et que le témoin ADSL est allumé.
2. Assurez-vous que vous avez entré les paramètres de VPI/VCI, de nom d'utilisateur et de mot de passe fournis par votre FAI.

Problème :

Ma connexion est de type « Adresse IP fixe ». Je n'arrive pas à me connecter sans fil à Internet.

Solution :

Puisque vous utilisez une adresse IP fixe, votre FAI doit vous attribuer l'adresse IP, l'adresse de masque de sous-réseau ainsi que l'adresse de la passerelle. Au lieu d'utiliser l'Assistant, allez à « Connection Type [Type de connexion] » et sélectionnez votre type de connexion. Cliquez « Next [Suivant] », sélectionnez « Static IP [IP fixe] », et entrez votre adresse IP, votre masque de sous-réseau et votre passerelle par défaut.

Problème :

J'ai oublié / j'ai perdu mon mot de passe.

Solution :

Appuyez sur le bouton de réinitialisation (à l'arrière du Routeur) et maintenez-le enfoncé pendant 10 secondes afin de rétablir les paramètres par défaut du fabricant.

Problème :

Mon PC sans fil n'arrive pas à se connecter au Routeur.

Solution :

1. Assurez-vous que PC sans fil possède le même SSID que le Routeur, et que les paramètres de sécurité (WPA et WEP) sont identiques sur chaque client et sur le Routeur.
2. Assurez-vous que la distance entre le Routeur et le PC sans fil n'est pas trop grande.

Problème :

Ma connexion au réseau sans fil est souvent interrompue.

Solution :

1. Déplacez votre PC sans fil plus près de votre Routeur, afin d'obtenir un meilleur signal.
2. Il y a peut-être beaucoup d'interférences, causées peut-être par un four à micro-ondes ou un téléphone sans fil 2,4 GHz. Déplacez le Routeur ou utilisez un canal différent.

Problème :

Je n'arrive pas à me connecter sans fil à Internet.

Solution :

Si vous n'arrivez pas à vous connecter à l'Internet à partir d'un ordinateur sans fil, veuillez vérifier les points suivants :

1. Observez les témoins sur votre Routeur. Si vous utilisez un Routeur Belkin, es témoins devraient ressembler à f ceci :
   - Le témoin d'alimentation doit être allumé.
   - Le témoin « DSL » doit être allumé, et ne doit pas clignoter.
   - Le témoin « Internet »» doit être allumé ou clignoter.
2. Lancez le logiciel de l'utilitaire sans fil en cliquant sur l'icône dans la barre de tâches, à l'angle inférieur droit de l'écran. Si vous utilisez une carte réseau sans fil Belkin, l'icône ressemble à ceci.  L'icône peut être rouge ou verte.
3. L'allure générale de la fenêtre qui s'ouvre dépend du modèle de la carte réseau que vous possédez. Toutefois,n'importe quel utilitaire doitposséder une liste de « Available Networks [Réseaux Disponibles] »,— les réseaux auxquels elle peut se connecter.

Est-ce que le nom de votre réseau apparaît dans la liste des réseaux disponibles ?

Oui, le nom de mon réseau apparaît – allez à la section intitulée « Je ne peux me connecter sans fil à l'Internet mais mon réseau apparaît dans la liste ».

Non, le nom de mon réseau n'apparaît pas - allez à la section intitulée « Je ne peux me connecter sans fil à l'Internet et mon réseau n'apparaît pas dans la liste ».

Problème :

Je ne peux me connecter sans fil à l'Internet mais mon réseau apparaît dans la liste.

Solution :

Si le nom de réseau apparaît dans la liste des réseaux disponibles, veuillez suivre les étapes suivantes afin de vous connecter sans fil :

1. Cliquez sur le nom de réseau valide dans la liste des réseaux disponibles.
2. Si le réseau est sécurisé (chiffrement), vous devrez entrer la clé réseau. Pour plus d'informations sur la sécurité, rendez vous à la page intitulée « Modification des paramètres de sécurité sans fil ».
3. Dans les secondes qui suivent, l'icône de la barre de tâches, à l'angle inférieur droit de l'écran, tournera au vert, indiquant une connexion au réseau.



Problème :

Je ne peux me connecter sans fil à l'Internet et mon réseau n'apparaît pas dans la liste.

Solution

Si le nom de votre réseau n'apparaît pas dans la liste des réseaux disponibles dans l'utilitaire, veuillez vérifier les points suivants :

1. Déplacez l'ordinateur, autant que possible, afin qu'il soit situé de 1,5 à 3 mètres du Routeur. Fermez l'utilitaire de réseau sans fil, et rouvrez-le. Si le nom de votre réseau sans fil apparaît maintenant dans la liste des réseaux disponibles, il se peut que

votre problème soit dû à la portée ou à une interférence. Veuillez consulter l'Appendice B à propos des « Facteurs à considérer pour le choix de l'emplacement et l'installation ».

2. À l'aide d'un ordinateur connecté au Routeur sans fil ou au point d'accès via un câble réseau (et non pas sans fil), assurez-vous que la « Broadcast SSID [Diffusion du SSID] » est activée. Ce paramètre se trouve dans l'onglet de configuration du Canal et du SSID du routeur sans fil.

Si vous ne pouvez toujours pas accéder à l'Internet après avoir vérifié les points précédents, veuillez contacter l'assistance technique de Belkin.

Problème :

Mon réseau sans fil ne fonctionne pas toujours.

Le transfert de données est parfois très lent.

La force du signal est faible.

J'éprouve des difficultés à établir/maintenir une connexion de type VPN (Virtual Private Network).

Solution :

La technologie sans fil est basée sur des ondes radio. Ceci implique que les performances et le débit de transfert entre les appareils diminuent lorsque ceux-ci sont éloignés les uns des autres. D'autres facteurs peuvent engendrer une dégradation du signal : le métal en est généralement responsable. Des obstacles tels des murs et des appareils métalliques peuvent aussi affecter la qualité du signal. Ainsi, à l'intérieur, la portée de vos appareils sans fil va de 30 à 60 mètres. Prenez note que la vitesse de connexion diminue également si vous vous éloignez du Routeur sans fil ou du point d'accès.

Afin de déterminer si vos problèmes de connexion sans fil sont dus à la portée, déplacez temporairement votre ordinateur dans un rayon d'environ 1,5 à 3 mètres de votre Routeur.

Modification du canal sans fil - Selon le trafic de données et les interférences au niveau local, passer à un autre canal peut améliorer la performance de votre réseau. Le canal par défaut de votre Routeur est 11. Vous pouvez choisir à partir de plusieurs autres canaux, dépendamment de votre région. Consultez la page 37 - « Modification du canal sans fil » pour de plus amples informations concernant le choix du canal.

Limiter le débit de données sans fil - Limiter le débit de données sans fil peut améliorer la portée sans fil maximale et la stabilité de la connexion. La plupart des cartes sans fil sont en mesure de limiter le débit de transmission. Pour modifier cette propriété, allez au Panneau de Configuration de Windows, ouvrez les Connexions Réseau et double-cliquez sur la connexion sans fil de votre carte. Dans la boîte de dialogue Propriétés, sélectionnez le bouton « Configure [Configurer] » à partir de l'onglet « Général ». (Les utilisateurs de Windows 98SE devront sélectionner la carte sans fil à partir de la liste, et cliquer ensuite sur Propriétés.) Choisissez ensuite l'onglet « Advanced [Avancé] » et sélectionnez la propriété « Rate [Débit] ». Les cartes clients sans fil sont habituellement configurées de façon à ajuster automatiquement le débit de transmission. Toutefois, ceci peut mener à des déconnexions périodiques lorsque le signal sans fil est trop faible. De façon générale, les débits de transmission plus lents sont plus stables. Faites des expériences avec différents débits de transmission jusqu'à ce que vous trouviez celui qui convient à votre environnement. Veuillez noter que chaque débit de transmission est acceptable pour naviguer sur Internet. Pour de plus amples informations, consultez le manuel de l'utilisateur de votre carte sans fil.

Problème :

J'éprouve des difficultés dans la configuration du Wired Equivalent Privacy (WEP) sur mon Routeur ou mon Point d'Accès Belkin.

Solution

1. Connectez-vous à votre Routeur ou votre Point d'Accès Sans Fil.
2. Ouvrez votre navigateur web et entrez l'adresse IP du Routeur ou du Point d'Accès Sans Fil. (L'adresse par défaut du Routeur est 192.168.2.1 et celle du Point d'Accès est 192.168.2.254.) Appuyez sur le bouton « Login [Connexion] », situé au coin supérieur droit du clavier, pour vous connecter au Routeur. Un message vous demande d'entrer votre mot de passe. Si vous n'avez pas encore créé un mot de passe personnalisé, laissez ce champ vide et cliquez sur « Submit [Envoyer] ».
3. Cliquez sur l'onglet « Wireless [Sans Fil] » à la gauche de votre écran. Cliquez sur l'onglet « Encryption [chiffrement] » ou « Security [Sécurité] » pour accéder à la page des paramètres de sécurité.
4. Sélectionnez « WEP 128 bits » dans le menu déroulant.
5. Après avoir sélectionné le mode de chiffrement WEP, vous pouvez entrer votre clé hexadécimale WEP manuellement ou vous pouvez entrer une phrase de passe dans le champ « Passphrase [Phrase de passe] » et cliquer sur « Generate [Générer] » pour créer la clé WEP à

partir de la phrase de passe. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres. Une clé hexadécimale est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP 128 bits, vous devez entrer 26 caractères hexadécimaux.

Par exemple :

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = clé 128 bits

6. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Le chiffrement de votre Routeur sans fil est maintenant configuré. Chaque ordinateur de votre réseau sans fil devra maintenant être configuré avec les mêmes paramètres de sécurité.

AVERTISSEMENT : Si vous configurez le Routeur Sans Fil ou le Point d'Accès à partir d'un ordinateur doté d'un client sans fil, vous devez vous assurer que la sécurité est ACTIVÉE pour ce client sans fil. Sinon, vous perdez votre connexion sans fil.

Remarque aux utilisateurs de Mac : Les produits AirPort® d'Apple ne prennent en charge que le chiffrement sur 64 bits. Les produits Apple AirPort 2 prennent en charge le chiffrement sur 64 bits ou 128 bits. Veuillez vérifier la version de votre produit Apple Airport. Si vous ne parvenez pas à configurer le réseau avec le chiffrement sur 128 bits, essayez sur 64 bits.

Problème :

J'éprouve des difficultés dans la configuration du Wired Equivalent Privacy (WEP) sur ma carte réseau.

Solution :

Votre Carte Réseau doit utiliser la même clé que votre Routeur ou Point d'Accès Sans Fil. Par exemple, si votre Routeur Sans Fil ou Point d'Accès utilise la clé 00112233445566778899AABBCC, votre carte réseau doit être paramétrée de façon à utiliser cette même clé.

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
2. Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
3. Ensuite, l'utilitaire LAN Sans Fil de Belkin apparaît. Cet Utilitaire vous permet d'accéder à toutes les fonctions avancées de votre carte réseau sans fil Belkin.
4. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Properties [Propriétés] ».

5. Sous « Data Encryption [Chiffrement de données] », sélectionnez « WEP ».
6. Assurez-vous que la case « The key is provided for me automatically [J'obtiens une clé automatiquement] » n'est pas cochée. Si vous utilisez cet ordinateur pour vous connecter à un réseau d'entreprise, prenez conseil auprès de votre administrateur réseau afin de savoir si cette case doit être cochée.
7. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

   Important : Une clé WEP est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP sur 128 bits, vous devez entrer 26 clés hexadécimales. Cette clé réseau doit être identique à la clé que vous avez assignée à votre Routeur ou Point d'Accès Sans Fil.

Par exemple : **C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4** = clé 128 bits

8. Cliquez sur « OK » et sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres.

Si vous utilisez une carte réseau sans fil **AUTRE** qu'une carte Belkin, consultez le manuel de l'utilisateur de votre carte sans fil.

Problème :

Est-ce que les produits Belkin prennent en charge le WPA ?

Solution

Remarque : Pour utiliser la sécurité par WPA, votre client doit être mis à jour avec les logiciels et les pilotes qui le prennent en charge. Au moment de mettre ce manuel sous presse, une rustine de sécurité est disponible pour téléchargement gratuit, auprès de Microsoft. Cette rustine ne fonctionne qu'avec Windows XP.

Vous pouvez télécharger la rustine ici :

http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

Vous devrez en outre télécharger le plus récent pilote pour votre Carte réseau sans fil 802.11g pour ordinateur de bureau ou portable de Belkin, que vous trouverez sur le site de l'assistance technique de Belkin. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment. La rustine de Microsoft ne prend en charge que les dispositifs avec pilotes compatibles WPA, tels que les produits 802.11g de Belkin.

Téléchargez le plus récent pilote à :
http://web.belkin.com/support/networkingsupport.asp.

La prise en charge WPA est installée automatiquement lorsque vous installez le Service Pack 2 de Windows XP. Pour plus d'informations : http://support.microsoft.com

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur mon Routeur ou mon Point d'Accès Sans Fil Belkin, pour mon réseau domestique.

Solution :

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA-PSK (no server) [sans serveur] ».
2. À « Encryption Technique [Technique de chiffrement] », choisissez « TKIP » ou « AES ». Ce paramètre devra être identique à celui des clients que vous configurerez.
3. Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres, symboles ou espaces). Cette clé doit être utilisée pour tous les clients branchés au réseau. Par exemple, votre clé pré-partagée peut ressembler à : « Clé réseau de la famille Dupont ».
4. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur mon Routeur ou mon Point d'Accès Sans Fil Belkin, pour mon réseau d'entreprise.

Solution :

Si votre réseau utilise un serveur Radius pour distribuer les clés aux clients, veuillez utiliser ce paramètre. Ce système se retrouve surtout en entreprise.

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA-PSK (no server) [sans serveur] ».
2. À « Encryption Technique [Technique de chiffrement] », choisissez « TKIP » ou « AES ». Ce paramètre devra être identique à celui des clients que vous configurerez.
3. Entrez l'adresse IP de votre serveur Radius dans le champ « Radius server [Serveur Radius] ».
4. Entrez la clé Radius dans le champ « Clé Radius ».
5. Entrez l'intervalle de clé. L'intervalle de clé correspond au nombre de fois où les clés sont distribuées (en paquets).
6. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur ma Carte Réseau Sans Fil Belkin, pour mon réseau domestique.

Solution :

Les clients doivent utiliser la même clé que le Routeur ou le Point d'Accès Sans Fil. Par exemple, si le Routeur ou le Point d'Accès Sans Fil est configuré avec la clé « Clé réseau de la famille Dupont », tous les clients doivent utiliser cette même clé.

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
2. Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
3. Ensuite, l'utilitaire LAN Sans Fil de Belkin apparaît. Cet Utilitaire vous permet d'accéder à toutes les fonctions avancées de votre carte réseau sans fil Belkin.
4. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Properties [Propriétés] ».
5. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA-PSK (No server) [WPA-PSK (Sans serveur)] ».
6. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

Important : Une clé WPA-PSK est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WPA-PSK, vous devez entrer de 8 à 63 caractères. Cette clé réseau doit être identique à la clé que vous avez assignée à votre Routeur ou Point d'Accès Sans Fil.

7. Cliquez sur « OK » et sur « Apply [Appliquer] » pour enregistrer les paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur ma Carte Réseau Sans Fil Belkin, pour mon réseau d'entreprise.

Solution :

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet

d'afficher et de configuration un plus grand nombre d'options de la carte.

2. Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
3. Ensuite, l'utilitaire LAN Sans Fil de Belkin apparaît. Cet Utilitaire vous permet d'accéder à toutes les fonctions avancées de votre carte réseau sans fil Belkin.
4. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Properties [Propriétés] ».
5. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA ».
6. Sous l'onglet « Authentication [Authentification] », choisissez les paramètres spécifiés par l'administrateur de votre réseau.
7. Cliquez sur « OK » et sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur ma Carte Réseau Sans Fil **AUTRE** que Belkin, pour mon réseau domestique.

Solution :

Pour les Cartes réseau sans fil pour ordinateurs de bureau ou portables **AUTRES** que Belkin et qui ne prenant pas en charge le WPA, une rustine de Microsoft, nommé « Windows XP Support Patch for Wireless Protected Access » est disponible pour téléchargement gratuit. Téléchargez la rustine de Microsoft en cherchant la base de connaissances avec « Windows XP WPA ».

Remarque : Cette rustine ne fonctionne qu'avec Windows XP. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment. Vous devrez en outre vous assurer que le fabricant de votre carte sans fil prend en charge le WPA et que vous avez téléchargé et installé le pilote le plus récent, que vous trouverez sur leur site web.

Systèmes d'exploitation pris en charge :

- Windows XP Professionnel
- Windows XP Édition Familiale

Pour activer le WPA-PSK (sans serveur)

1. Sous Windows XP, cliquez Démarrer > Panneau de Configuration > Connexions Réseaux et Internet .
2. En cliquant avec le bouton droit de votre souris sur « Réseaux Sans Fil », vous verrez une fenêtre s'afficher comme suit : Assurez-vous que la boîte « Use Windows to configure my wireless network settings [Utiliser Windows pour configurer mes paramètres réseau sans fil] » est cochée.

3. Sous l’onglet « Wireless Networks [Réseaux Sans Fil] », cliquez sur le bouton « Configure [Configurer] » et vous verrez une fenêtre s’afficher comme suit :

4. Pour l’utilisateur de réseau domestique ou de petite entreprise, sélectionnez « WPA-PSK » sous « Network Administration [Administration Réseau] ».

Remarque : Sélectionnez le WPA si vous utilisez cet ordinateur pour vous brancher à un réseau d’entreprise, qui à son tour prend en charge un serveur d’authentification tel que le serveur RADIUS. Renseignez-vous auprès de l’administrateur de votre réseau pour de plus amples informations.

5. Sélectionnez « TKIP » sous « Data Encryption [Chiffrement de données] ». Ce paramètre devra être identique à ce lui que vous configurerez sur le Routeur ou le Point d’Accès Sans Fil.

6. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

Important : Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres ou symboles). Cette clé doit être utilisée pour tous les clients branchés au réseau.

7. Cliquez « OK » pour enregistrer les paramètres.

Quelle est la différence entre 802.11b, 802.11g, G+ MIMO et Pre-N ?

À l’heure actuelle, il existe quatre normes de réseaux sans fil qui transmettent des données à des débits maximaux différents. Chaque norme est basée sur le radical 802.11(x), utilisé par la IEEE, l’organisme responsable de la certification des normes réseaux. La norme réseau la plus courante, le 802.11b, transmet les données à 11 Mbps. Les normes 802.11a, 802.11g, G+ MIMO transmettent à 54 Mbps. Le Pre-N, quand à lui, transmet à 108 Mbps.

Tableau comparatif des réseaux sans fil

Technologie sans fil	802.11b	G (802.11g)	G+ (802.11g avec HSM)	G+ MIMO(802.11g avec MIMO MRC)	Belkin Pre-N(802.11g avec True MIMO)
Débit*	Débit de liaison 11 Mbps	5x plus rapide que le 802.11b*	10x plus rapide que le 802.11b*	10x plus rapide que le 802.11b*	15x plus rapide que le 802.11b*
Fréquence	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz
Compatibilité	Compatible avec le 802.11g	Compat-ible avec : 802.11b/g	Compatible avec le 802.11b/g	Compatible avec le 802.11b/g	Compatible avec le 802.11g ou le 802.11b
Couver-ture*	Généralement 30 à 60 mètres à l'intérieur	Jusqu'à 120 mètres*	Jusqu'à 210 mètres*	Jusqu'à 300 mètres*	Jusqu'à 425 mètres*
Avantage	Ancien : technologie plus ancienne	Populaire : grande popularité pour le partage d'une connexion Internet	Meilleure couverture et débit plus rapide	Meilleure couverture avec débit plus stable	Technologie de pointe : le meilleur débit et la meilleure couverture

*La portée et le débit de la connexion dépendent de l'environnement de votre réseau.

Appendice A : Glossaire

Adresse IP

L’ « Adresse IP » représente l’Adresse IP interne du Routeur. Pour accéder à l’interface de configuration avancée, entrez cette adresse IP dans la barre d’adresse de votre navigateur. Cette adresse peut être modifiée au besoin. Pour modifier l’adresse IP, entrez la nouvelle adresse IP et cliquez sur « Apply Changes [Enregistrer les Modifications] ». L’adresse IP choisie doit être une adresse IP non-acheminable. Exemples d’adresses IP non-acheminables :

192.168.x.x (où x est un nombre compris entre 0 et 255)

10.x.x.x (où x est un nombre compris entre 0 et 255)

Masque de Sous-Réseau

Certains réseaux sont beaucoup trop élargis pour permettre à tout le trafic de submerger toutes ses parties. Ces réseaux doivent être divisés en en sections plus restreintes et facilement administrables : les sous-réseaux. Le masque de sous-réseau consiste en l’adresse du réseau, en plus de l’information réservée à l’identification du sous-réseau.

DNS

DNS est l'acronyme de Domain Name Server, qui se traduit par Serveur de Noms de Domaine. Un Serveur de Noms de Domaine est un serveur que l'on retrouve sur l'Internet et qui traduit les URL (Universal Resource Links), telles que www.belkin.com, en adresses IP. Cette information n'est pas requise de la plupart des FAI lors de la configuration du Routeur. Si vous êtes utilisez une connexion de type IP statique, vous pouvez avoir besoin de saisir une adresse DNS spécifique ainsi qu'une adresse DNS secondaire pour que votre connexion puisse fonctionner correctement. Si vous utilisez une connexion de type dynamique ou PPPoE, il est fort probable que vous n'ayez pas à entrer d'adresse DNS.

PPPoE

La plupart des fournisseurs de services ADSL utilisent la connexion de type PPPoE. Si vous utilisez un modem ADSL pour vous brancher à Internet, votre FAI utilise probablement le protocole PPPoE pour vous relier au service.

Vous possédez une connexion PPPoE si :

1. Votre FAI vous a attribué un nom d'utilisateur et un mot de passe, qui sont requis pour vous brancher à Internet.
2. Votre FAI vous a fourni des logiciels tels que WinPOET et Enternet300, et vous utilisez ceux-ci pour vous brancher à Internet,
3. Vous devez double-cliquer une icône sur votre bureau, autre que celle de votre navigateur, pour vous brancher à Internet.

   Pour configurer le Routeur selon le protocole PPPoE, entrez votre nom d'utilisateur et votre mot de passe dans les champs prévus. Après avoir entré les informations, cliquez sur « Apply Changes [Enregistrer les Modifications] ».

L'indicateur d'état de l'Internet affichera « Connexion OK » si votre Routeur est configuré de façon appropriée.

PPPoA

Entrez les informations relative au PPPoA dans les champs prévus, et cliquez sur « Next [Suivant] ». Cliquez sur « Apply [Appliquer] » pour que les paramètres soient pris en compte.

1. Nom d'utilisateur – Entrez le nom d'utilisateur. (Fourni par votre FAI.)
2. Mot de passe – Entrez votre mot de passe. (Fourni par votre FAI.)
3. Entrez à nouveau le mot de passe – Confirmer le mot de passe. (Fourni par votre FAI.)
4. VPI/VCI – Entrez ici vos paramètres de d'identificateur de trajet virtuel (VPI) et d'identificateur de voie virtuelle (VCI). (Fourni par votre FAI.)

Déconnecter après X...

Cette fonction permet de déconnecter automatiquement le Routeur de votre FAI, lorsque celui-ci est inactif pour une période de temps déterminée. Par exemple, si vous cochez cette option et que vous mettez « 5 » dans le champ des minutes, le Routeur se déconnectera de l'Internet après 5 minutes d'inactivité Internet. Cette option doit être utilisée si votre FAI vous facture à la minute.

Canal et SSID

Pour modifier le canal d'opération du Routeur, sélectionnez le canal désiré à partir de la liste déroulante et sélectionnez votre canal. Ensuite, cliquez sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres. Vous pouvez également modifier le SSID. Le SSID est l'équivalent du nom du réseau sans fil. Vous pouvez lui donner n'importe quel nom. S'il existe d'autres réseaux sans fil dans votre environnement immédiat, vous devez donner un nom unique au vôtre. Pour modifier le SSID, cliquez sur la zone SSID, puis entrez le nouveau nom. Cliquez sur « Apply Changes [Enregistrer les Modifications] » pour qu'elles soient prises en compte.

Diffusion de l'ESSID

Plusieurs adaptateurs réseau sans fil disponibles sur le marché à l'heure actuelle comprennent une fonction appelée ‘ analyse du site ‘. Cette fonction permet de balayer l'air ambiant à la recherche de n'importe quel réseau disponible, et permet à chaque ordinateur de sélectionner automatiquement un réseau parmi ceux-ci. C'est possible lorsque le SSID de l'ordinateur est paramétré avec « TOUS ». Votre Routeur Belkin permet le blocage de cette recherche de réseaux. Si vous désactivez la fonction « ESSID Broadcast [Diffusion d'ESSID] », le seul moyen dont dispose votre ordinateur pour se brancher au réseau est de paramétrer le SSID de celui-ci en lui donnant le nom spécifique du réseau (par exemple WLAN). Assurez-vous de connaître le SSID (nom du réseau) avant d'activer cette fonction. Il est possible de rendre presque invisible votre réseau sans fil. En désactivant l'émission du SSID, votre réseau n'apparaîtra pas lors de l'analyse du site. Il va de soi que désactiver la fonction de diffusion du SSID augmente le niveau de sécurité.

Chiffrement

Le chiffrement contribue à préserver la sécurité de votre réseau. Pour protéger vos données, le Routeur utilise le « Wired Equivalent Privacy » (WEP) et le « WiFi Protected Access » (WPA). Votre Routeur présente deux niveaux de chiffrement : 64 bits et 128 bits. Le chiffrement fonctionne avec

un système de clés. La clé de l'ordinateur doit correspondre à la clé du Routeur. On peut créer une clé de deux façons. La façon la plus simple consiste à laisser le logiciel du Routeur convertir en clé une phrase de passe que vous avez entrée. Une méthode plus avancée consiste à entrer la clé manuellement.

Serveurs Virtuels

Cette fonction vous permet d'acheminer, via le Routeur et vers votre réseau interne, les appels externes (Internet) de services tels qu'un serveur web (port 80), un serveur FTP (port 21) ou d'autres applications. Parce que vos ordinateurs internes sont protégés par le pare-feu, les machines provenant de l'Internet ne peuvent accédez à ceux-ci puisqu'ils sont invisibles . Si vous devez configurer la fonction de Serveur Virtuel pour une application particulière, vous devez contacter le fabricant de votre application et déterminer quels paramètres de ports sont nécessaires.

Pour entrer les paramètres manuellement, entrez l'adresse IP dans l'espace prévu pour la machine (serveur) interne, les ports public et LAN requis pour la passerelle. Sélectionnez ensuite « Enable [Activer] » et cliquez sur « Set [Établir] ». Vous pouvez uniquement faire passer un seul port par adresse IP interne. L'ouverture des ports de votre pare-feu risque de compromettre la sécurité de votre réseau. Vous pouvez rapidement activer ou désactiver cette fonction. Il est recommandé de désactiver cette fonction lorsque vous n'utilisez pas d'application spécifique.

Filtres d'IP des clients

Le Routeur peut être configuré de sorte à limiter l'accès de certains ordinateurs à Internet, au courrier électronique et autres fonctions réseaux, à des jours et des heures donnés. La restriction peut s'appliquer à un seul ordinateur, à un groupe d'ordinateurs ou à plusieurs ordinateurs.

Filtrage des adresses MAC

Le filtrage d'adresses MAC est une fonction de sécurité puissante qui vous permet de spécifier les ordinateurs autorisés à se connecter au réseau. Tout ordinateur non spécifié dans les paramètres du filtre et qui tente d'accéder au réseau se verra refuser l'accès. Lorsque vous activez cette fonction, vous devez entrer l'adresse MAC de chaque client de votre réseau, pour permettre à chacun d'accéder au réseau, ou copier l'adresse MAC en sélectionnant le nom de l'ordinateur à partie de la Liste de clients DHCP . Si vous souhaitez activer cette fonction, sélectionnez l'option Activer . Ensuite, cliquez sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres.

Zone DMZ

Si un de vos PC clients ne peut éxécuter une application Internet convenablement parce qu'il se trouve derrière un pare-feu, vous pouvez modifier les restrictions en permettant l'accès à internet bidirectionnel. Cette opération peut s'avérer nécessaire si la traduction d'adresse réseau (NAT) empêche le bon fonctionnement d'applications telles que les jeux ou les vidéoconférences. Servez-vous de cette fonction au besoin. **L'ordinateur placé dans la zone DMZ ne sera pas protégé contre les attaques provenant de hackers.**Pour placer un ordinateur dans la zone DMZ, entrez les derniers chiffres de son adresse IP de réseau local dans le champ de saisie d'IP Statique, et cliquez sur « Apply Changes [Enregistrer les Modifications] » pour que celles-ci soient prises en compte.

Si vous n'avez qu'une adresse IP publique (WAN), vous pouvez laisser l'IP publique à « 0.0.0.0 ». Si vous utilisez plusieurs adresses IP (WAN) publiques, il est possible de sélectionner vers quelle adresse IP (WAN) publique l'hôte DMZ sera dirigé. Entrez l'adresse IP (WAN) publique vers laquelle vous désirez diriger l'hôte DMZ, entrez les deux derniers chiffres de l'adresse IP de l'ordinateur hôte de la zone DMZ, choisissez Activer et cliquez sur « Apply Changes [Enregistrer les Modifications] ».

Mot de passe Administrateur

Le Routeur est livré SANS mot de passe défini. Si par souci de sécurité vous désirer ajouter un mot de passe, vous pouvez le configurer à partir de l'interface basée sur navigateur Web de votre Routeur. Conservez votre mot de passe dans un endroit sûr, puisque vous aurez besoin de ce mot de passe lorsque vous voudrez vous connecter au Routeur par la suite. Il est **FORTEMENT RECOMMANDÉ** d'ajouter un mot de passe si vous prévoyez utiliser la fonction de gestion à distance du Routeur. L'option de temporisation de la connexion vous permet de déterminer une plage horaire pendant laquelle vous pouvez être connecté à l'interface de configuration avancée du Routeur. La temporisation débute lorsqu'il n'y a plus d'activité. Par exemple, vous avez apporté des modifications au niveau de l'interface de configuration évoluée, puis vous avez quitté l'ordinateur sans cliquer sur « Logout [Déconnexion] ».

En prenant pour exemple un temporisateur paramétré à 10 minutes, votre connexion prendra fin 10 minutes après votre départ. Vous devrez donc vous connecter à nouveau au Routeur pour apporter d'autres modifications. L'option de temporisation de la connexion sert à des fins de sécurité, et le paramètre par défaut est 10 minutes. À titre de remarque, un seul ordinateur à la fois peut être connecté à l'interface de configuration avancée du Routeur.

Définition d'un fuseau horaire

Le Routeur harmonise le temps en se connectant à un serveur SNTP (Simple Network Time Protocol). Ceci lui permet de synchroniser l'horloge du système avec l'Internet planétaire. L'horloge ainsi synchronisée est utilisée par le routeur pour garder un journal de connexions et pour contrôler le filtrage des clients. Sélectionnez le fuseau horaire du pays dans lequel vous résidez. Si vous résidez dans une région qui applique l'horaire d'été, cochez la case près de l'option « Enable Daylight Saving [Appliquer les horaires d'été] ». L'horloge du système peut ne pas être mise à jour immédiatement. Laissez au minimum 15 minutes au Routeur pour contacter les serveurs horaires sur Internet et obtenir une réponse.

Gestion à distance

Avant d'activer cette fonction, **ASSUREZ-VOUS D'AVOIR AJOUTÉ UN MOT DE PASSE ADMINISTRATEUR**. La gestion à distance vous permet d'apporter des changements aux paramètres de votre Routeur, où que vous soyez grâce à l'Internet.

UPnP

L'UPnP (Universal Plug-and-Play) est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux, et d'autres applications compatibles avec l'UPnP. Certaines applications nécessitent que le pare-feu du Routeur soit configuré selon certains paramètres pour fonctionner adéquatement. Pour ce faire, vous devez habituellement ouvrir des ports TCP et UDP et, parfois, définir des ports de déclenchement. Une application qui est compatible avec l'UPnP possède la capacité de communiquer avec le Routeur, lui indiquant la façon dont le pare-feu doit être configuré. Le routeur est livré avec la fonction UPnP désactivée. Si vous utilisez une application qui est compatible avec l'UPnP, et si vous désirez bénéficier des avantages de l'UPnP, vous pouvez activer la fonction UPnP. Choisissez simplement « Enable [Activer] » dans la partie « UPnP Enabling [Activation UPnP] » de la page « Utilities [Utilitaires] ». Cliquez sur « Apply Changes [Enregistrer les modifications] » pour enregistrer les modifications.

Appendice B : Facteurs à considérer pour l'installation et la mise en route

Remarque : Alors que certains des objets énumérés ci-dessous peuvent affecter les performances de votre réseau, ils n'empêcheront pas son fonctionnement. Si vous croyez que votre réseau sans fil ne fonctionne pas à pleine capacité, ces solutions peuvent vous aider.

1. **Choix de l'emplacement de votre Routeur ou votre Point d'Accès sans fil**

   Placez votre Routeur Réseau Sans Fil (ou Point d'Accès), le centre nerveux de votre réseau sans fil, aussi près que possible du centre de la zone de couverture désirée.

   Afin d'assurer une zone de couverture optimale pour vos « clients réseau » (soit les ordinateurs dotés d'une carte réseau pour ordinateur de bureau ou portable ou d'un adaptateur USB de Belkin) :

   - Assurez-vous que les antennes de votre routeur sans fil (ou de votre point d'accès) sont parallèles et disposées à la verticale (en pointant vers le plafond). Si votre Routeur (ou votre Point d'Accès) est posé à la verticale, essayez autant que possible de disposer les antennes de façon à ce qu'elles pointent vers le haut.
   - Dans des habitations à plusieurs étages, placez le Routeur (ou le Point d'Accès) à l'étage le plus central de votre domicile. Ceci peut signifier que devrez placer le Routeur sans fil (ou le Point d'Accès) à un étage supérieur
   - Évitez de placer le Routeur (ou le Point d'Accès) près d'un téléphone sans fil 2.4 GHz.

2. **Éviter les obstacles et les interférences**

   Évitez de placer le Routeur ou le Point d'Accès près d'un appareil émettant des ondes radio, comme un four à micro-ondes. Exemples d'objets denses pouvant empêcher la communication sans fil :

   - Réfrigérateurs
   - Lave-linge et/ou sèche-linge
   - Étagère en métal
   - Grands aquariums
   - Fenêtres teintées (contre les UV) à base de métal

Si le signal de votre réseau semble faible à certains endroits, assurez-vous qu'aucun de ces objets ne peut lui faire obstruction (entre les ordinateurs et le routeur ou le point d'accès).

3. **Téléphones sans fil**

Si les performances de votre réseau sans fil sont toujours affectées malgré les solutions mentionnées ci-dessus et si vous possédez un téléphone sans fil :

- Éloignez votre téléphone de votre Routeur ou votre Point d'Accès sans fil ainsi que de vos ordinateurs sans fil.
- Débranchez et retirez la batterie de tout téléphone sans fil fonctionnant sur la bande de 2.4 GHz. (Consultez la documentation accompagnant votre téléphone à cet effet.) Si ces gestes semblent résoudre le problème, c'est que votre téléphone interfère avec les signaux du réseau sans fil.
- Si votre téléphone prend en charge la sélection du canal, modifiez le canal de votre téléphone en choisissant autant que possible le canal le plus éloigné du canal de votre réseau sans fil. Par exemple, choisissez le canal 1 pour votre téléphone et modifiez le canal de votre Routeur ou de votre Point d'Accès en choisissant le canal 11. Consultez la documentation accompagnant votre téléphone pour de plus amples informations.
- Si le besoin se fait sentir, vous pouvez aussi changer votre téléphone sans fil en choisissant un téléphone à 900 MHz ou à 5 GHz.

4. **Choisissez le canal le plus « paisible » pour votre réseau sans fil**

Dans des environnements domiciliaires ou d'entreprise rapprochés, tels que les appartements et les immeubles à bureaux, il se peut qu'un autre réseau sans fil interfère et entre en conflit avec votre réseau.

Grâce à la fonction d'analyse du site de l'Utilitaire de réseau sans fil, vous pourrez localiser d'autres réseaux sans fil disponibles (consultez le manuel de votre adaptateur sans fil), et choisir pour votre Routeur sans fil (ou Point d'Accès) un canal aussi loin que possible du canal utilisé par ces réseaux.

Essayez plusieurs canaux parmi ceux disponibles afin de déterminer la connexion la plus claire et éviter les interférences de la part de téléphones sans fil ou d'autres dispositifs sans fil se trouvant dans votre voisinage.

1 2 3 4 5 6 7 8 9 10 section

Pour les dispositifs de réseau sans fil d’une marque différente, utilisez la fonction d’analyse de site détaillée et consultez les informations concernant les canaux qui se trouvent dans ce manuel.

Ces solutions devraient vous permettre d’obtenir une zone de couverture maximale avec votre Routeur ou votre Point d’Accès. Si vous devez étendre votre zone de couverture, nous vous suggérons le Point d’accès/Module d’extension de Belkin.

5. Connexions sécurisées, VPN et AOL

Une connexion sécurisée est une connexion qui requiert un nom d’utilisateur et un mot de passe et qui est utilisée là où la sécurité revêt une grande importance. Parmi les connexions sécurisées :

- Les connexions de type Virtual Private Network (VPN - réseau privé virtuel), souvent utilisées pour accéder à distance à un réseau d’entreprise
- Le programme Bring your own access d’America Online (AOL) qui vous permet d’utiliser AOL via une connexion à large bande (DSL ou câble) offerte par un autre fournisseur d’accès à Internet.
- La plupart des banques en ligne
- Plusieurs sites commerciaux qui requièrent un nom d’utilisateur et un mot de passe afin d’accéder à un compte

Les connexions sécurisées peuvent être interrompues par les paramètres de gestion de l’énergie de votre ordinateur (lorsqu’il est en état de veille). La solution la plus simple afin d’éviter cette situation est de vous reconnecter en lançant le logiciel de VPN ou d’AOL ou en vous reconnectant via le site web sécurisé.

Une solution alternative consiste à changer les paramètres de gestion de l’énergie afin qu’il ne soit plus mis en état de veille. Toutefois, cette solution peut ne pas être appropriée pour les ordinateurs portables. Pour modifier les paramètres de gestion de l’énergie de Windows, rendez-vous à « Power Options [Options d’alimentation] », dans le « Control Panel [Panneau de Configuration] ».

Si les difficultés reliées aux connexions sécurisées, au VPN et à AOL persistent, veuillez relire les étapes 1 à 4 ci-dessus afin de vous assurer d’avoir tenté les solutions proposées.

Appendice C : Tableau des paramètres Internet

L’information contenue dans le tableau suivant sert de référence à propos des paramètres de connexion ADSL de votre FAI. Plusieurs FAI utilisent des paramètres différents, selon la région et l’équipement utilisé. Essayez d’abord les paramètres appropriés pour votre région. S’ils ne fonctionnent pas, communiquez avec votre FAI pour les paramètres spécifiques.

Pays	Protocole de connexion	VPI/VCI	Encapsulation	FAI
Europe				
France	PPPoE	8/35	LLC	Divers
Allemagne	PPPoE	1/32	LLC	T-Online, divers autres
Pays-Bas	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Divers
Belgique	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italie	PPPoE ou PPPoA	8/35	VC MUX	TIN
Espagne	PPPoE ou 1483 Bridged	8/32	LLC	Telefonica
Suède	1483 Bridged	3/35	LLC	Telia
Royaume-Uni	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Asia				
Australie	PPPoE ou PPPoA	8/35	LLC	Divers
Nouvelle-Zélande	PPPoE ou PPPoA	0/100	VC MUX	Divers
Singapour	PPPoE	0/100	LLC	SingNet, Pacific Internet

Déclaration FCC

DÉCLARATION DE CONFORMITÉ À LA RÉGLEMENTATION FCC EN MATIÈRE DE COMPATIBILITÉ ÉLECTROMAGNÉTIQUE

Nous, Belkin Corporation, sis au 501 West Walnut Street, Compton CA, 90220, États-Unis, déclarons sous notre seule responsabilité que le produit

F5D9630-4

auquel se réfère la présente déclaration,
est conforme aux normes énoncées à l'alinéa 15 de la réglementation FCC. Le fonctionnement est assujetti aux deux conditions suivantes : (1) cet appareil ne peut pas provoquer d'interférence nuisible et (2) cet appareil doit accepter toute interférence reçue, y compris des interférences pouvant entraîner un fonctionnement non désiré.

Attention : La puissance d'émission en sortie de cet appareil reste largement en dessous des limites d'exposition aux fréquences radios de la FCC. Toutefois, il est conseillé d'utiliser l'appareil de manière à minimiser les risques d'exposition dans des conditions de fonctionnement normales.

Lorsqu'une antenne extérieure est raccordée à l'appareil, la placer de manière à minimiser les risques d'exposition dans des conditions de fonctionnement normales. Pour éviter la possibilité d'excéder les limites d'exposition aux fréquences radio de la FCC, il est conseillé d'éviter qu'une personne se trouve à moins de 20 cm de l'antenne dans des conditions de fonctionnement normales.

Avertissement de la Commission Fédérale des Communications (FCC)
L'appareil a été testé et satisfait aux limites de la classe B des appareils numériques, conformément à l'alinéa 15 de la réglementation FCC. Ces limites sont conçues de manière à assurer une protection raisonnable contre les interférences nuisibles au sein d'une installation domestique.

L'appareil génère, utilise et peut irradier une énergie radiofréquence. Si cet équipement cause des interférences nuisibles sur le plan de la réception radio ou télévision, pouvant être déterminées en mettant l'appareil sous et hors tension, l'utilisateur est invité à tester et à corriger l'interférence en prenant une des mesures suivantes :

- Réorienter ou changer de place l'antenne de réception.
- Augmenter la distance entre l'appareil et le récepteur.
- Connecter l'appareil à une prise située sur un circuit différent de celui sur lequel le récepteur est connecté.
- Consulter le revendeur ou un technicien en radio/TV.

Modifications
La réglementation de la FCC souligne la nécessité d'indiquer à l'utilisateur que toute modification, de quelque nature que ce soit et non agréée par Belkin Corporation, lui retire le droit d'utiliser l'appareil.

Canada-Industrie Canada (IC)
La radio sans fil de cet appareil est conforme aux normes RSS 139 & RSS 210 d'Industrie Canada. This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Europe - Prescription Union européenne
Les produits radio portant le label CE 0560 ou CE alert satisfont à la directive R&TTE (1995/5/CE) établie par la Commission de la Communauté européenne.

L'accord avec cette directive implique la conformité aux normes européennes suivantes (la norme internationale équivalente est indiquée entre parenthèses).

- EN 60950 (IEC60950) - Sécurité des produits
- EN 300 328 Conditions techniques exigées pour les appareils radio
- ETS 300 826 Conditions générales en matière de compatibilité électromagnétique pour les appareils radio.

Prière de consulter la plaque d'identification apposée sur votre produit Belkin pour déterminer le type d'émetteur.

Les produits portant le label CE satisfont à la directive relative à la compatibilité électromagnétique (89/336/EEC) et la directive sur les basses tensions (72/23/EEC) publiées par la Commission de la Communauté européenne. La conformité avec ces normes sous-entend la conformité avec les normes européennes suivantes (le standard international équivalent est indiqué entre parenthèses).

- EN 55022 (CISPR 22) - Interférences électromagnétiques
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Immunité électromagnétique
- EN 61000-3-2 (IEC610000-3-2) – Émissions de courants harmoniques
- EN 61000-3-3 (IEC610000) - Fluctuations de tension et flicker
- EN 60950 (IEC60950) - Sécurité des produits

Les produits équipés de transmetteurs radio portent la marque CE 0560 ou CE alert et peuvent également afficher le logo CE.



La présence de ce symbole sur le produit ou sur son emballage indique que vous ne pouvez pas vous débarasser de ce produit de la même façon que vos déchets ménagers. Au contraire, vous êtes responsable de l'élimination de vos équipements usagés et à cet effet, vous êtes tenu de les remettre à un point de collecte agréé pour le recyclage des équipements électriques et électroniques usagés. La collecte et le recyclage de vos équipements usagés permettent de préserver les ressources naturelles et de s'assurer que ces équipements sont recyclés dans le respect de la santé humaine et de l'environnement. Pour connaître les lieux de collecte des équipements usagés aux fins de recyclage, veuillez contacter votre mairie, votre service de traitement des déchets ménagers ou le magasin où vous avez acheté le produit.

Garantie limitée à vie du produit de Belkin Corporation

Belkin Corporation garantit ce produit contre tout défaut matériel ou de fabrication pendant toute sa durée de vie. Si l'appareil s'avère défectueux, Belkin le réparera ou le remplacera gratuitement, à sa convenance, à condition que le produit soit retourné, port payé, pendant la durée de la garantie, au dépositaire Belkin agréé auprès duquel le produit a été acheté. Une preuve d'achat peut être exigée.

La présente garantie est caduque si le produit a été endommagé par accident, abus, usage impropre ou mauvaise application, si le produit a été modifié sans autorisation écrite de Belkin, ou si un numéro de série Belkin a été supprimé ou rendu illisible.

LA GARANTIE ET LES VOIES DE RECOURS SUSMENTIONNÉES FONT FOI EXCLUSIVEMENT ET REMPLACENT TOUTES LES AUTRES, ORALES OU ÉCRITES, EXPLICITES OU IMPLICITES. BELKIN REJETTE EXPRESSÉMENT TOUTES LES GARANTIES IMPLICITES, Y COMPRIS MAIS SANS RESTRICTION, LES GARANTIES AFFÉRENTES À LA QUALITÉ LOYALE ET MARCHANDE ET À LA POSSIBILITÉ D'UTILISATION À UNE FIN DONNÉE.

Aucun dépositaire, représentant ou employé de Belkin n'est habilité à apporter des modifications ou adjonctions à la présente garantie, ni à la proroger.

BELKIN N'EST PAS RESPONSABLE DES DOMMAGES SPÉCIAUX, DIRECTS OU INDIRECTS, DÉCOULANT D'UNE RUPTURE DE GARANTIE, OU EN VERTU DE TOUTE AUTRE THÉORIE JURIDIQUE, Y COMPRIS MAIS SANS RESTRICTION LES PERTES DE BÉNÉFICES, TEMPS D'ARRÊT, FONDS DE COMMERCE, REPROGRAMMATION OU REPRODUCTION DE PROGRAMMES OU DE DONNÉES MÉMORISÉS OU UTILISÉS AVEC DES PRODUITS BELKIN OU DOMMAGES CAUSÉS À CES PROGRAMMES OU À CES DONNÉES.

Certains pays ne permettent pas d'exclure ou de limiter les dommages accidentels ou consécutifs ou les exclusions de garanties implicites, de sorte que les limitations d'exclusions ci-dessus ne s'appliquent pas dans votre cas. La garantie vous confère des droits légaux spécifiques. Vous pouvez également bénéficier d'autres droits qui varient d'un pays à l'autre.

Modem ADSL2+ avec Routeur Sans Fil G+ MIMO

Vous trouverez des informations techniques sur le site www.belkin.com dans la zone d'assistance technique.

Pour communiquer avec le service d'assistance technique par téléphone, veuillez composer le numéro apparaissant dans la liste ci-dessou

*Hors coût de communication nationale

Assistance technique gratuite*

AUTRICHE	08 - 20 20 07 66	LUXEMBOURG	34 20 80 8560
RÉPUBLIQUE TCHÈQUE	23 900 04 06	PAYS-BAS	0900 - 040 07 90
DANEMARK	701 22 403	NORVÈGE	815 00 287
FINLANDE	00800 - 22 35 54 60	POLOGNE	00800 - 441 17 37
FRANCE	08 - 25 54 00 26	PORTUGAL	707 200 676
ALLEMAGNE	0180 - 500 57 09	RUSSIE	495 580 9541
GRÈCE	00800 - 44 14 23 90	AFRIQUE DU SUD	0800 - 99 15 21
HONGRIE	06 - 17 77 49 06	ESPAGNE	902 - 02 43 66
ISLANDE	800 8534	SUÈDE	07 - 71 40 04 53
IRLANDE	0818 55 50 06	SUISSE	08 - 48 00 02 19
ITALIE	02 - 69 43 02 51	ROYAUME-UNI	0845 - 607 77 87

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220-5221, États-Unis
310-898-1100
310-898-1111 Fax

Belkin Ltd.
7 Bowen Crescent, West Gosford
NSW 2250, Australie
+61 (0) 2 4372 8600
+49 (0) 89 1434 05-0 Fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Royaume-Uni
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 Fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Pays-Bas
+31 (0) 20 654 7300
+31 (0) 20 654 7349 Fax

P75125ea_A

BELKIN

ADSL2+ Modem mit kabellosem G+ MIMO Router

Vernetzen Sie Ihre Computer und nutzen Sie den ADSL-Internetanschluss gemeinsam

UK
FR
DE
NL
ES
IT



Benutzerhandbuch

802.11g
G+
MIMO

F5D9630de4A

Inhaltsverzeichnis

Einleitung

Wir beglückwünschen Sie zum Kauf dieses ADSL-Modems mit integriertem kabellosem Hi-Speed Router. In wenigen Minuten können Sie Ihren Internet-Zugang gemeinsam nutzen und Ihre Computer zu einem Netzwerk verbinden. Die folgende Liste beinhaltet die Merkmale, die Ihren Router zur idealen Lösung für Ihr Netzwerk zu Hause oder in einem kleinen Büro machen. Bitte lesen Sie dieses Handbuch sorgfältig durch und beachten Sie besonders den Anhang B mit dem Titel „Wichtige Faktoren bei Aufstellung und Einrichtung".

Vorzüge eines Netzwerks zu Hause

Wenn Sie unseren einfachen Konfigurationsanleitungen folgen, können Sie Ihr Belkin-Netzwerk zu Hause folgendermaßen einsetzen:

- Nutzung einer Hi-Speed Internetverbindung mit allen Computern bei Ihnen zu Hause
- Nutzung von Ressourcen wie Dateien und Festplatten auf allen angeschlossenen Computern bei Ihnen zu Hause
- Nutzung eines einzigen Druckers mit der ganzen Familie
- Gemeinsamer Zugriff auf Dokumente, Musik, Video und digitale Fotos
- Speichern von Dateien auf verschiedenen Computern; Aufrufen und Kopieren dieser auf verschiedenen Computern
- Gleichzeitiges Spielen von Internetspielen, Verschicken und Empfangen von E-Mails und Chatten

Vorteile eines kabellosen Netzwerks von Belkin

Mobilität – Sie brauchen kein spezielles „Computerzimmer" mehr - Sie können jetzt überall in der Reichweite des kabellosen Netzwerks an einem vernetzten Notebook oder Desktop-Computer arbeiten

Einfache Installation – Der Installations-Assistent von Belkin vereinfacht die Konfiguration

Flexibilität – Sie können Drucker, Computer und andere Netzwerkgeräte überall zu Hause aufstellen und benutzen

Einfache Erweiterung – Die große Palette an Netzwerkprodukten von Belkin ermöglicht die Erweiterung Ihres Netzwerks mit Geräten wie Druckern und Spielkonsolen

Keine Verkabelung erforderlich – Sie können sich Kosten und Mühe für die Aufrüstung der Ethernetverkabelung im ganzen Haus oder Büro sparen

Breite Akzeptanz auf dem Markt – wählen Sie aus einem großen Angebot an Netzwerkprodukten aus, die vollständig kompatibel sind

Sie benötigen Folgendes

Verpackungsinhalt

- ADSL2+ Modem mit kabellosem G+ MIMO Router
- RJ11 Telefonschnur - Grau
- RJ45 Ethernet-Netzwerkkabel - Gelb
- ADSL-Mikrofilter*
- Netzteil
- Benutzerhandbuch auf CD

*ADSL-Mikrofilter (Splitter) sind landesspezifisch. Ist dieser nicht vorhanden, müssen Sie einen erwerben.

Systemvoraussetzungen

- Ein aktiver ADSL-Dienst mit einem Telefonanschluss zur Verbindung mit dem Router
- Mindestens ein richtig konfigurierter Computer mit einer Netzwerkkarte (Network Interface Card - NIC) und installiertem Browser.
- TCP/IP-Netzwerkprotokoll auf jedem Computer installiert, der mit dem Router verbunden ist
- Kein anderer DHCP-Server in Ihrem lokalen Netzwerk, der Computern und Geräten IP-Adressen zuteilt

Internet-Verbindungseinstellungen

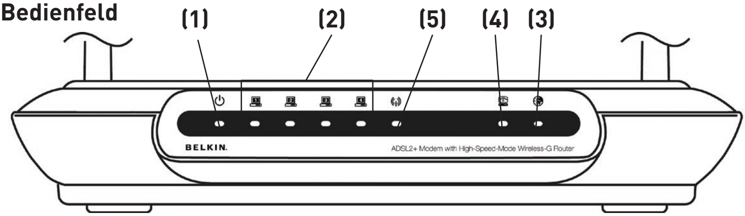
Bitte erfragen Sie bei Ihrem Internetanbieter erst die folgenden Informationen, bevor Sie den kabellosen ADSL-Modemrouter einstellen.

- Internet-Verbindungsprotokoll: ________ (PPPoE, PPPoA, Dynamic IP, Static IP)
- Methode: Multiplexing oder Kapselung: _________ (LLC oder VC MUX)
- Virtueller Circuit: VPI (Virtual Path Identifier) _________ (eine Zahlzwischen 0 und 255)
- VCI (Virtual Channel Identifier) _________ (eine Zahlzwischen 1 und 65535)
- Für PPPoE- und PPPoA-Nutzer: ADSL-Konto-Benutzername ____________ und Kennwort ______________
- Für Nutzer einer statischen IP-Adresse: IP-Adresse ___ . ___ . ___ . ___
  Subnet Mask ___ . ___ . ___ . ___
  Standard Gateway-Server ___ . ___ . ___ .
- IP-Adresse für Domänennamen-Server ___ . ___ . ___ . ___ (von Internetanbieter zugeteilt)

Hinweis: Beachten Sie den Anhang C in diesem Handbuch. Dort finden Sie einige gebräuchliche Parameter für die DSL-Interneteinstellungen. Wenn Sie sich der Einstellungen nicht sicher sind, wenden Sie sich bitte an Ihren Internetanbieter.

Der Router kann auf den Schreibtisch gestellt werden. Alle Kabel sind an der Rückseite des Routers angeschlossen, um eine ordentliche Installation zu erleichtern. Die LED-Anzeigen sind gut sichtbar an der Router-Vorderseite angebracht, so dass Sie Status und Aktivität des Netzwerks jederzeit ablesen können.

Bedienfeld



1. Betriebsanzeige

Wenn Sie den Router einschalten oder neu starten, dauert es einige Sekunden, bis der Router hochfährt. Wenn der Router vollständig hochgefahren ist, leuchtet die Betriebsanzeige GRÜN auf und zeigt damit an, dass der Router betriebsbereit ist.

	AUS	Router ist AUS.
	Grün	Router ist AN
	Rot	Router konnte nicht gestartet werden

2. LAN-Statusanzeigen

Diese Leuchten sind mit 1-4 nummeriert. Die Nummern entsprechen den Schnittstellen auf der Router-Rückseite. Wenn ein Computer korrekt mit einer der LAN-Schnittstellen an der Router-Rückseite verbunden ist, leuchtet die Anzeige auf. Eine GRÜN leuchtende Anzeige zeigt an, dass ein netzwerkfähiges Gerät mit dem Netzwerk verbunden ist. Wenn Daten über die Schnittstelle übertragen werden, blinkt die LED in schneller Folge auf. ORANGE bedeutet, dass eine 10Base-T-Verbindung aktiv ist.

	AUS	Kein Gerät ist verbunden
	Orange	Die Ethernetverbindung ist aktiv und ein 10Base-T-Gerät ist verbunden
	Orange (Blinkanzeige)	Datenübertragung eines 10Base-T-Geräts
	Grün	Die Ethernetverbindung ist aktiv und ein 10Base-T-Gerät ist verbunden
	Grün (Blinkanzeige)	Datenübertragung eines 100Base-T-Geräts

3. **WLAN-Statusanzeige**

Die WLAN-Statusanzeige leuchtet GRÜN, wenn die kabellose LAN-Verbindung steht. Die Anzeige blinkt, wenn der Router Daten kabellos überträgt.

AUS	WLAN ist nicht aktiv
Grün	WLAN ist aktiv
Grün (Blinkanzeige)	Bei Datenübertragung

4. **ADSL-Anzeige**

Die ADSL-Anzeige blinkt während der Prüfung der Verbindung zu Ihrem Internet-Provider GRÜN. Sie bleibt GRÜN, wenn der Router eine ADSL-Verbindung hergestellt hat.

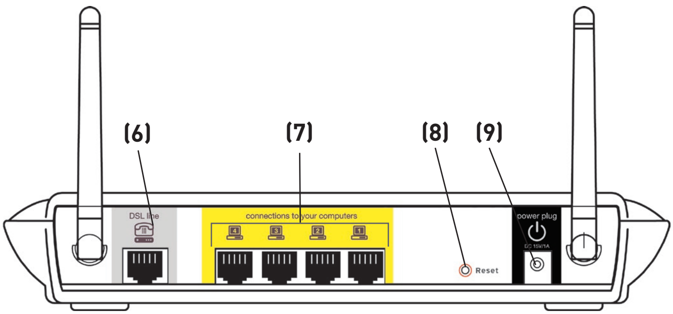
AUS	Keine ADSL-Verbindung
Grün	ADSL-Verbindung aktiv
Grün (Blinkanzeige)	Verbindungsprüfung

5. **Internet-Anzeige**

Die Internet-Anzeige zeigt an, ob der Router mit dem Internet verbunden ist. Ist die Anzeige AUS, besteht KEINE Verbindung. Leuchtet die Anzeige GRÜN auf, ist der Router mit dem Internet verbunden. Wenn die Anzeige blinkt, empfängt oder versendet der Router Daten aus dem oder in das Internet.

AUS	Keine Internetverbindung
Grün	Verbunden mit dem Internet
Grün (Blinkanzeige)	Bei Datenübertragung
Rot	IP-Adresse nicht erhalten

Rückseite



6. **DSL-Leitung**
   Dieser Anschluss dient zur Verbindung mit der ADSL-Leitung. Verbinden Sie das ADSL-Kabel mit diesem Anschluss.

7. **Ethernet-Ports**
   Die Ethernet-Ports sind RJ45-Anschlüsse mit 10/100 Auto-Negotiation. Die Ports sind mit den Zahlen 1 bis 4 bezeichnet, die mit den nummerierten LED-Lampen an der Vorderseite des Routers übereinstimmen. Verbinden Sie Ihre Netzwerk-Computer oder andere Netzwerkgeräte mit einem dieser Ports.

8. **Rücksetztaste**
   Die Rücksetztaste wird nur in seltenen Fällen benötigt, wenn der Router nicht mehr korrekt funktioniert. Beim Zurücksetzen wird der Router in den Normalbetrieb versetzt. Die programmierten Einstellungen bleiben erhalten. Mit der Rücksetztaste können Sie auch die Werkseinstellungen wiederherstellen. Dies ist zum Beispiel nützlich, wenn Sie das von Ihnen eingestellte Kennwort vergessen haben.

   a. **Zurücksetzen des Routers**
      Halten Sie die Rücksetztaste eine Sekunde lang gedrückt. Wenn die Betriebs-/Bereitschaftsanzeige wieder Dauerlicht anzeigt, ist das Zurücksetzen abgeschlossen.

   b. **Wiederherstellen der Werkseinstellungen**
      Halten Sie die Rücksetztaste fünf Sekunden lang gedrückt. Wenn die Betriebs-/Bereitschaftsanzeige wieder Dauerlicht anzeigt, ist die Wiederherstellung abgeschlossen.

9. **Netzanschluss**
   Schließen Sie das enthaltenen 15V-DC-Netzteil an diesen Anschluss an. Die Verwendung eines falschen Adaptertyps kann zu Schäden am Router führen.

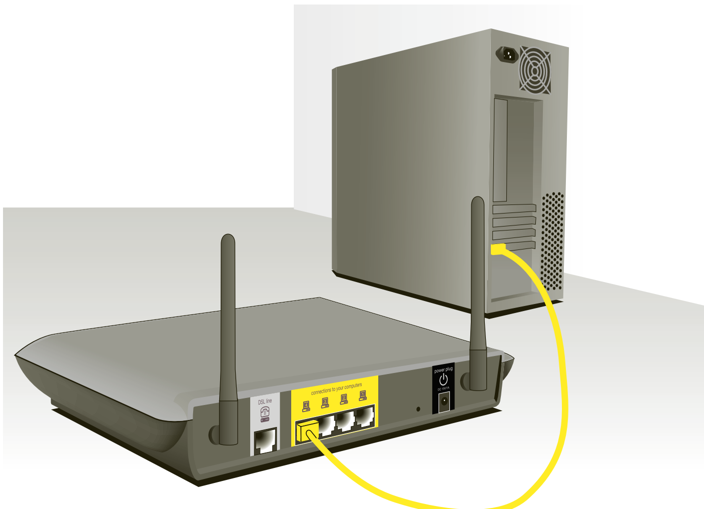
Aufstellung des Routers

Je näher Ihr Computer an Ihrem Router steht, desto stärker ist Ihre kabellose Verbindung. Die durchschnittliche Reichweite für Ihre kabellosen Geräte liegt zwischen 30 und 60 Metern. Entsprechend wird Ihre kabellose Verbindung und Leistung sich etwas verschlechtern, wenn Sie den Abstand zwischen Ihrem kabellosen Router und den angeschlossenen Geräten vergrößern. Das kann Ihnen möglicherweise auffallen. Wenn Sie sich von Ihrem Router oder Access Point entfernen, kann sich die Verbindungsgeschwindigkeit unter Umständen verringern. Geräte aus Metall oder Wände und andere Hindernisse sind Faktoren, die die Signale möglicherweise abschwächen, da Sie die Funkwellen Ihres Netzwerks durch Ihre bloße Anwesenheit stören können. Beachten Sie hierzu den Anhang B: „Wichtige Faktoren bei Aufstellung und Einrichtung” in diesem Handbuch.

Um zu überprüfen, ob die Leistung Ihres Netzwerks durch die Reichweite oder Hindernisse negativ beeinflusst wird, versuchen Sie Ihren Computer in einem Abstand von 1,5 bis 3 m vom kabellosen Router aufzustellen. Dann werden Sie sehen, ob eventuelle Probleme aufgrund des Abstands auftreten. Wenn Verbindungsschwierigkeiten auch bei kurzer Distanz zum Router auftreten, beachten Sie bitte das Kapitel „Fehlerbehebung”.

Anschließen der Computer

1. Schalten Sie Computer und Netzwerkgeräte aus.
2. Verbinden Sie Ihren Computer mit einem der GELBEN RJ45-Ports mit der Aufschrift „connections to your computers" (Verbindung zu den Computern) an der Rückseite des Routers. Verwenden Sie dazu ein Ethernet-Netzwerkkabel (im Lieferumfang erhalten).



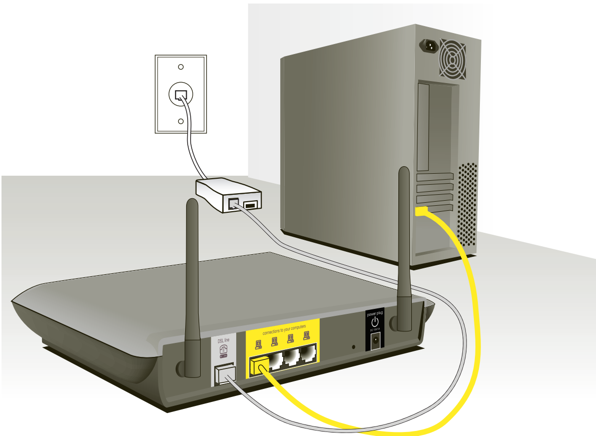
Verbindung mit der ADSL-Leitung

Die Verbindung des Routers mit der ADSL-Verbindung ist landesspezifisch. Normalerweise wird dazu ein Mikrofilter mit oder ohne integrierten Splitter verwendet, um die gleichzeitige Verwendung von ADSL-Diensten und Telefon über eine Leitung zu ermöglichen. Bitte lesen Sie die folgenden Schritte aufmerksam durch und wählen Sie die für Sie geeignete Anschlussmethode.

1. Wenn Ihr Telefon- und Ihr ADSL-Anschluss über ein und dieselbe Telefonleitung geführt werden, benötigen Sie ADSL-Mikrofilter (Splitter) für jedes Telefon und jedes weitere Gerät wie Anrufbeantworter, Faxgeräte oder Nummern-Anzeigen. Weitere Splitter können nötig sein, um für Telefon und Router unterschiedliche Telefonleitungen zu verwenden.

   Hinweis: Verbinden Sie den ADSL-Mikrofilter nicht mit dem Telefonanschluss und dem Router—dadurch wird verhindert, dass der ADSL-Service das Modem erreicht.

2. Wenn Ihr Telefon- und Ihr ADSL-Service über eine Telefonleitung geführt werden und Sie einen ADSL-Mikrofilter mit integriertem Splitter verwenden, schließen Sie den Splitter an die Telefonbuchse an, über die der ADSL-Service angeboten wird. Verbinden Sie dann die Telefonschnur mit dem ADSL-Mikrofilterport RJ11, meist mit „DSL" beschriftet, und dem grauen Router-Port RJ11, mit „DSL line" (DSL-Leitung) beschriftet, der sich an der Rückseite Ihres Routers befindet. Verbinden Sie das Telefon mit dem anderen Port am ADSL-Splitter, der meist mit „Telefon" beschriftet ist. Ein weiterer ADSL-Mikrofilter wird benötigt, wenn Sie ein weiteres Telefon oder ein anderes Gerät über dieselbe Leitung verwenden.



Hinweis: Eine RJ11-Telefonschnur ist im Lieferumfang enthalten. Achten Sie darauf, dass der Stecker in der Wandsteckdose fest einrastet.

3. Wenn Sie eine bestimmte ADSL-Leitung mit einem RJ11-Anschluss haben, verbinden Sie die Telefonleitung einfach mit demgrauen RJ11-Anschluss „DSL-Leitung" an der Rückseite des Routers.

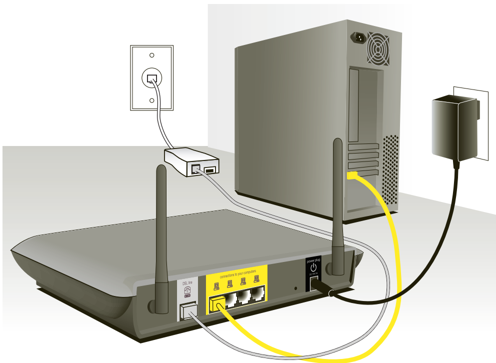
4. Wenn Sie eine RJ45-Dose für Ihren ADSL-Service haben, schließen Sie einen RJ45/RJ11-Konverter an diese Dose an. Verbinden Sie dann eine Telefonschnur mit diesem Konverter und dem grauen RJ11-Anschluss „DSL-Leitung" an der Rückseite des Routers.

Hinweis:ADSL-Mikrofilter werden nicht in allen Ländern angeboten.

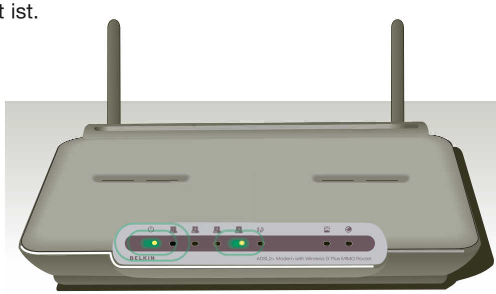
Anschalten des Routers

1. Verbinden Sie das mitgelieferte Netzteil mit dem Netzausgang des Routers. Dieser ist mit „Power” beschriftet.

   Hinweis: Verwenden Sie aus Sicherheitsgründen nur das mitgelieferte Netzteil, um Schäden am Router zu vermeiden.



2. Wenn nach dem Anschluss an die Stromquelle die Geräte eingeschaltet werden, sollte die Betriebsanzeige des Routers.⏻ an der Vorderseite des Geräts an sein. Es kann ein paar Minuten dauern, bis der Router vollständig gestartet ist.



3. Schalten Sie die Computer ein. Nachdem Sie Ihren Computer gestartet haben, leuchtet die LAN-Statusanzeige 💻 an der Vorderseite des Routers für jeden Port, mit dem ein verkabelter Computer verbunden ist. Diese Anzeigen signalisieren Verbindung und Aktivität. Jetzt können Sie den Router für die ADSL-Verbindung konfigurieren.

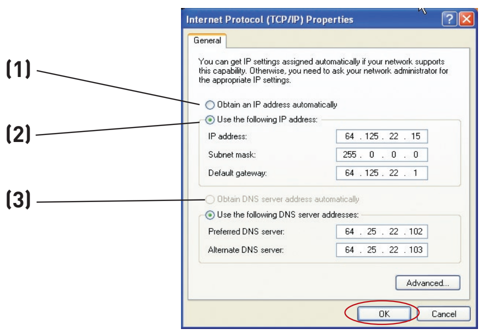
Damit Ihr Computer korrekt mit dem Router kommunizieren kann, müssen Sie die TCP/IP-Einstellungen Ihres Computers auf „Obtain an IP address automatically/Using DHCP” (DNS-Serveradresse automatisch beziehen) ändern. Dies ist bei den meisten PCs in der Regel als Standard voreingestellt.

Richten Sie den Computer, der mit dem DSL-Modem verbunden ist, ZUERST mit den folgenden Schritten ein. Auf die gleiche Weise können Sie weitere Computer zum Router hinzufügen, nachdem der Router für die Internet-Verbindung konfiguriert wurde.

Manuelles Konfigurieren des Netzwerkadapters unter Windows XP, 2000 oder NT

1. Klicken Sie auf Start, Einstellungen, Systemsteuerung.

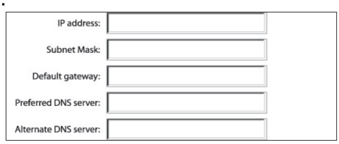
2. Doppelklicken Sie auf das Symbol „Network and dial-up connections” (Netzwerk- und DFÜ-Verbindungen öffnen) (Windows 2000) bzw. „Network” (Netzwerk) (Windows XP).



3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung Ihres Netzwerkadapters und wählen Sie „Properties” (Eigenschaften) aus dem Dropdown-Menü.

4. Im Fenster „LAN-Verbind ungseigenschaften” klicken Sie „Internet Protocol (TCP/IP)” und dann die Schaltfläche „Eigenschaften”. Daraufhin wird das folgende Fenster geöffnet:

5. Wenn „Use the following IP address” (Folgende IP-Adresse verwenden)**(2)** ausgewählt ist, muss Ihr Router für eine statische IP-Verbindung eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.



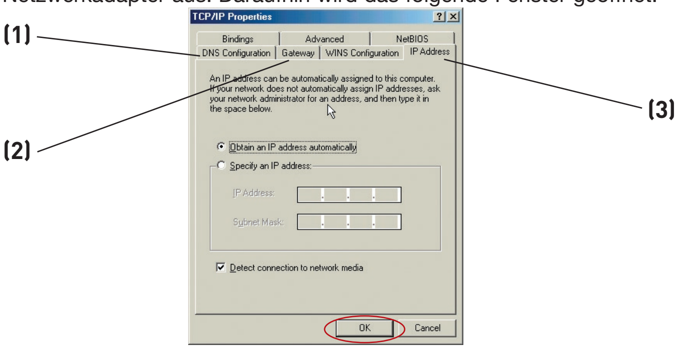
6. Wählen Sie „Obtain an IP address automatically” (IP-Adresse automatisch beziehen) **(1)** und „Obtain DNS server address automatically” (DNS-Serveradresse automatisch beziehen), wenn diese Punkte noch nicht ausgewählt sind.**(3)**. Klicken Sie auf „OK”.

Ihre Netzwerkadapter werden jetzt für den Gebrauch mit dem Router konfiguriert.

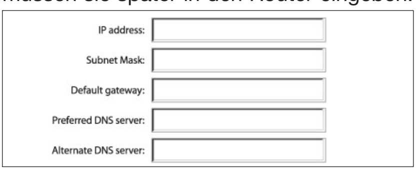
Manuelle Konfiguration der Netzwerkadapter unter Windows 98SE oder ME

1. Klicken Sie mit der rechten Maustaste auf „Netzwerkumgebung”, und wählen Sie „Eigenschaften” aus dem Dropdown-Menü.

2. Wählen Sie die Option „TCP/IP > Einstellungen” für den installierten Netzwerkadapter aus. Daraufhin wird das folgende Fenster geöffnet.



3. Wenn die Option „Specify an IP address” (IP-Adresse festlegen) ausgewählt ist, muss der Router für einen statischen IP-Verbindungstyp eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.



IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

4. Notieren Sie sich die in der Registerkarte IP-Adresse angegebene IP-Adresse und Subnet Mask **(3)**.

5. Klicken Sie auf die Registerkarte „Gateway” **(2)**. Notieren Sie die Gateway-Adresse in der Tabelle.

6. Klicken Sie auf die Registerkarte „DNS Configuration” (DNS-Konfigurierung)**(1)**. Notieren Sie die DNS-Adresse(n) in der Tabelle.

7. Soweit noch nicht geschehen, aktivieren Sie auf der Registerkarte IP-Adresse die Option „IP-Adresse automatisch beziehen.” Klicken Sie auf „OK”.

8. Für eine korrekte Konfiguration und eine reibungslose Verbindung mit dem Router müssen Sie zudem die Gateway-Adresse auf der Registerkarte Gateway und bei den Einträgen unter DNS-Konfiguration entfernen.

Starten Sie den Computer neu. Während des Neustarts werden Ihre Netzwerkadapter für den Gebrauch mit dem Router konfiguriert.

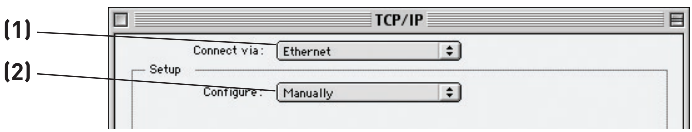
Richten Sie den Computer, der mit dem Kabel- oder DSL-Modem verbunden ist, ZUERST mit den folgenden Schritten ein. Auf die gleiche Weise können Sie weitere Computer zum Router hinzufügen, nachdem der Router für die Internet-Verbindung konfiguriert wurde.

Manuelles Konfigurieren der Netzwerkeinstellungen in Mac OS bis Version 9.x

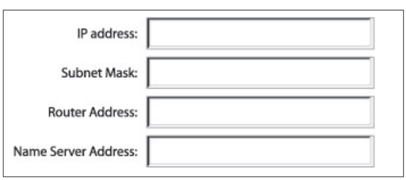
Damit Ihr Computer korrekt mit dem Router kommunizieren kann, müssen Sie die TCP/IP-Einstellungen Ihres Mac-Computers zu DHCP ändern.

1. Öffnen Sie das Applemenü. Wählen Sie „Control Panels” (Kontrollfelder) > „TCP/IP”.

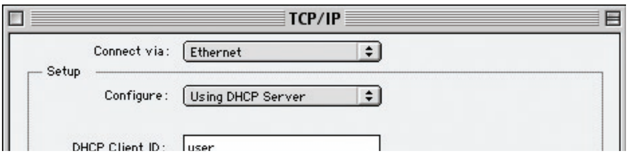
2. Die TCP/IP-Kontrollfelder werden angezeigt. Wählen Sie unter „Connect Via:” (Verbindung:) entweder „Ethernet Built In” (Ethernet integriert) oder „Ethernet” **(1)**.



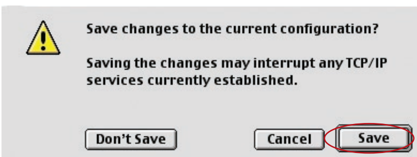
3. Wenn bei „Configure” (Konfigurationsmethode)**(2)**„Manuell” ausgewählt ist, muss der Router für eine statische IP-Verbindung eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.



4. Soweit noch nicht unter „Configure” (Konfigurationsmethode) eingestellt, wählen Sie die Option „Using DHCP Server” (Über DHCP-Server). Dadurch wird der Computer angewiesen, eine IP-Adresse vom Router anzufordern.



5. Schließen Sie das Fenster. Wenn Sie Änderungen vorgenommen haben, erscheint das folgende Fenster. Klicken Sie auf „Save” (Sichern).



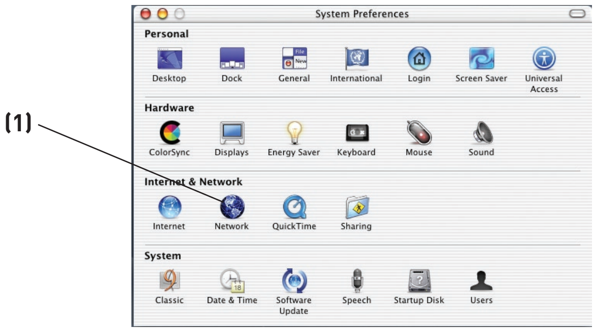
Starten Sie den Computer neu. Während des Neustarts werden die Netzwerkeinstellungen für den Router konfiguriert.

Manuelles Konfigurieren der Netzwerkadapter unter Mac OS X

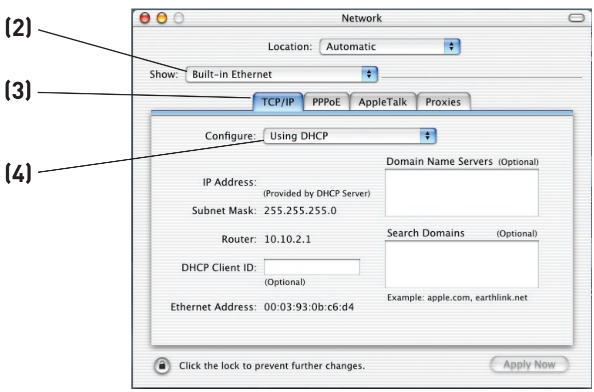
1. CKlicken Sie auf das Symbol „System Preferences” (Systemeinstellungen).



2. Wählen Sie das Symbol „Network” **(1)** (Netzwerk) unter „System Preferences” (Systemeinstellungen) aus.

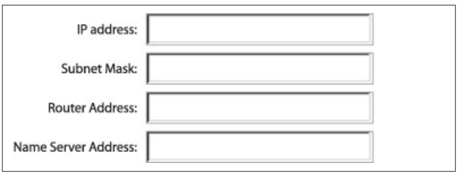


3. Wählen Sie unter „Network” (Netzwerk) „Built-in Ethernet” (Ethernet integriert)**(2)** neben „Show” (Zeigen).



4. Wählen Sie die Registerkarte „TCP/IP" **(3)**. Neben „Configure" **(4)**(Konfigurieren) müsste „Manually" (Manuell) oder „Using DHCP" (über DHCP) angezeigt werden. Wenn nicht, vergewissern Sie sich, dass auf der Registerkarte „PPPoE" **(5)** „PPPoE verwenden" NICHT ausgewählt ist. Ist dies der Fall, müssen Sie den Router mittels Benutzername und Kennwort für einen PPPoE-Verbindungstyp konfigurieren.

5. Wenn die Option „Manually" (Manuell) ausgewählt ist, muss der Router für einen statischen IP-Verbindungstyp eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.

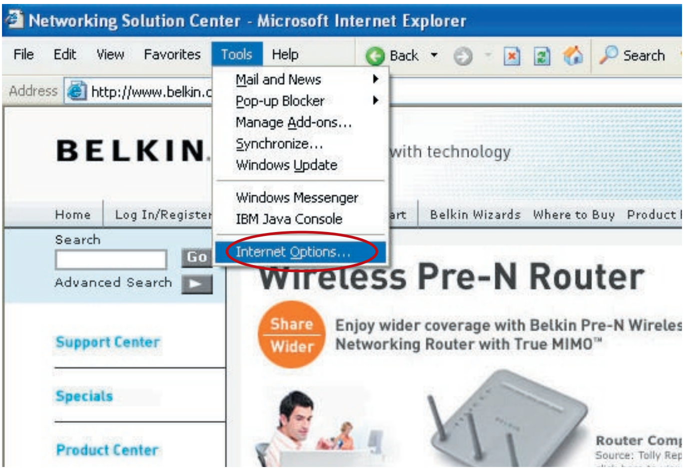


6. Soweit noch nicht geschehen, wählen Sie neben „Configure" **(4)**„Using DHCP" (DHCP verwenden) und klicken Sie auf „Apply Now" (Jetzt anwenden).

Ihre Netzwerkadapter werden jetzt für den Gebrauch mit dem Router konfiguriert.

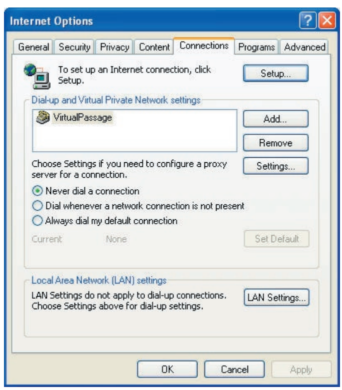
Empfohlene Browser-Einstellungen

Normalerweise können Sie die Browser-Einstellungen unverändert lassen. Wenn es beim Zugriff auf das Internet oder die Erweiterte Benutzeroberfläche zu Problemen kommt, können Sie jedoch auf die empfohlenen Einstellungen in diesem Abschnitt zurückgreifen.



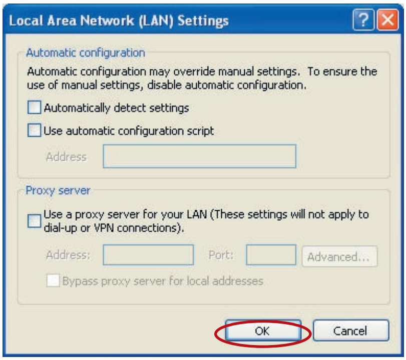
Internet Explorer 4.0 (oder höher)

1. Starten Sie Ihren Webbrowser. Wählen Sie „Extras" und die Funktion „Internetoptionen".
2. m Fenster Internetoptionen stehen drei Optionen zur Auswahl: „Keine Verbindung wählen", „Nur wählen, wenn keine Netzwerkverbindung besteht" und „Immer Standardverbindung wählen". Wenn die Optionen verfügbar sind, aktivieren Sie „Keine Verbindung wählen". Wenn die Optionen nicht verfügbar sind, fahren Sie mit dem nächsten Schritt fort.



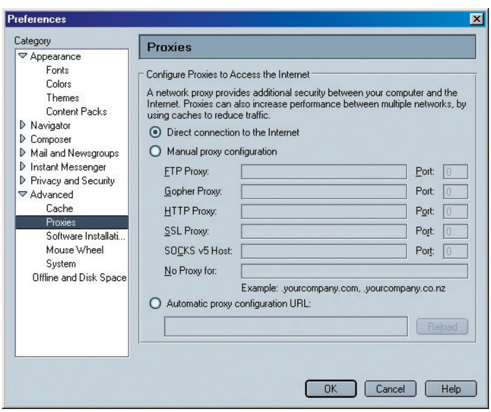
3. Klicken Sie auf die Registerkarte „Verbindungen", und wählen Sie „LAN-Einstellungen...".

4. Stellen Sie sicher, dass keine der folgenden Optionen aktiviert ist: „Automatische Suche der Einstellungen”, „Automatisches Konfigurationsskript verwenden” sowie „Einen Proxyserver verwenden”. Klicken Sie auf „OK”. Klicken Sie im Dialogfeld „Internetoptionen” abermals auf „OK”.



Netscape Navigator 4.0 (oder höher)

1. Starten Sie Netscape. Klicken Sie auf „Bearbeiten” > „Einstellungen”.
2. Klicken Sie im Dialogfeld Einstellungen auf „Erweitert” und dann auf „Proxies”. Klicken Sie im Dialogfeld „Proxies” auf „Direkte Verbindung zum Internet”.



Konfigurieren des Routers mit dem Konfigurationsassistenten

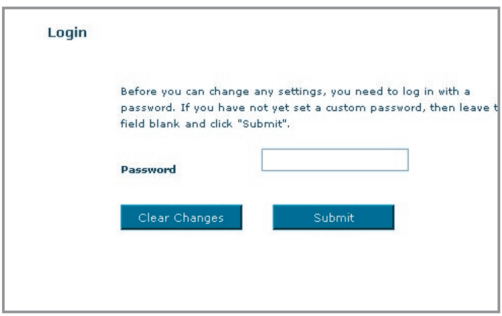
Ausführen des Konfigurationsassistenten

1. Sie können auf die Webbasierte Benutzeroberfläche mit einem Internetbrowser zugreifen, wenn der entsprechende Computer mit dem Router verbunden ist. Geben Sie in die Adresszeile des Browsers „192.168.2.1" ein. (Lassen Sie alle weiteren Angaben wie „http://" und „www" weg). Drücken Sie dann die Eingabetaste.



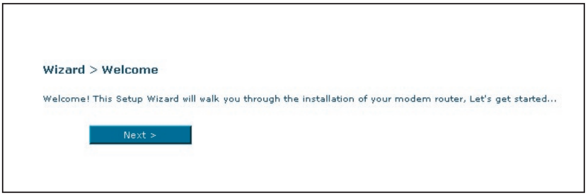
Hinweis: Wir empfehlen nachdrücklich, dass Sie für die erste Einrichtung einen Computer verwenden, der über ein Kabel (RJ45) mit dem Router verbunden ist. Es ist nicht empfehlenswert, dafür einen Computer mit Funkverbindung zum Router zu verwenden.

2. Über das folgende Fenster im Browser werden Sie aufgefordert, sich anzumelden. Der Router wird ohne festgelegtes Kennwort geliefert. Lassen Sie die Kennwortzeile auf dem Anmeldefenster leer, und klicken Sie auf „Submit" (Absenden), um sich anzumelden.

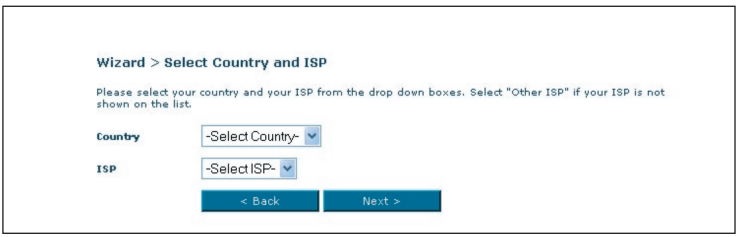


Hinweis: Wir empfehlen nachdrücklich, dass Sie im Sinne einer erhöhten Sicherheit ein neues Kennwort einstellen. Bitte lesen Sie das folgende Kapitel mit dem Titel „Manuelle Konfiguration des Routers" aufmerksam durch.

3. Der Konfigurationsassistent startet automatisch die Schnellkonfiguration (empfohlen). Klicken Sie auf „Next” (Weiter), um fortzufahren.



4. Wählen Sie erst Ihr Land und Ihren Internet-Provider aus und klicken Sie dann auf „Next” (Weiter). Wenn Ihr Land und/oder Ihr Internet-Provider nicht aufgeführt werden, wählen Sie „Other Country” (Anderes Land) oder „Other ISP” (Anderer Internet-Provider)



5. Geben Sie jetzt Benutzernamen und Kennwort, die Sie von Ihrem Internet-Provider erhalten haben, in die leeren Felder ein. Es ist wichtig, dass Benutzername und Kennwort korrekt eingegeben werden, da die Verbindung ansonsten nicht hergestellt werden kann. Ihr Internet-Provider kann Ihnen Benutzernamen und Kennwort bestätigen.



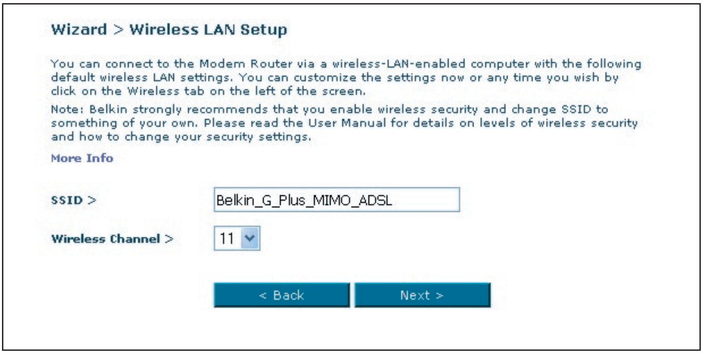
Hinweis: Eine detaillierte Anleitung für weitere Verbindungstypen finden Sie im Kapitel „Manuelle Konfiguration des Routers” in diesem Handbuch.

6. Jetzt wird das WLAN-Konfigurierungsfenster angezeigt. Sie können auch über einen WLAN-fähigen Computer eine Verbindung zum Router herstellen. Verwenden Sie dazu die folgenden Standard-WLAN-Einstellungen:

   SSID = Belkin G+ MIMO ADSL

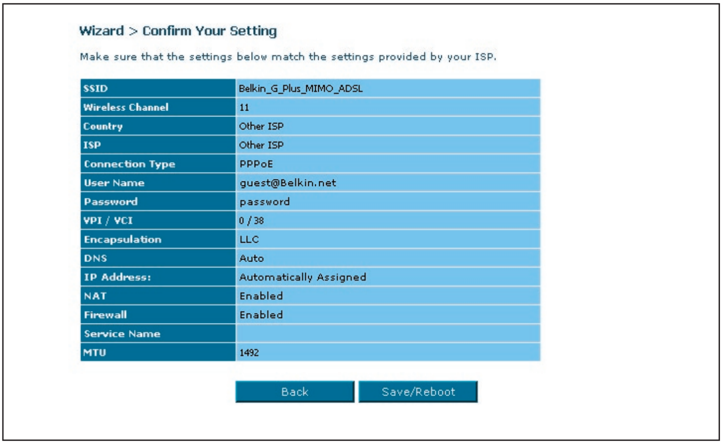
   Wireless Channel (Funkkanal) = Auto

   Security = off (Sicherheit = aus)



Hinweis: Belkin empfiehlt nachdrücklich, dass Sie die Funksicherheitsfunktion WEP oder WPA aktivieren und die SSID auf einen Namen Ihrer Wahl ändern. Im Benutzerhandbuch finden Sie weitere Informationen über Sicherheitsebenen von Funkverbindungen und über deren Einstellung.

7. Überprüfen Sie die Einstellungen, die im folgenden Fenster angezeigt werden. Sie können auf „Back" (Zurück) klicken, um die Einstellungen zu ändern. Andernfalls klicken Sie auf „Next" (Weiter), um die Einstellungen zu bestätigen.



Wizard > Confirm Your Setting

Make sure that the settings below match the settings provided by your ISP.

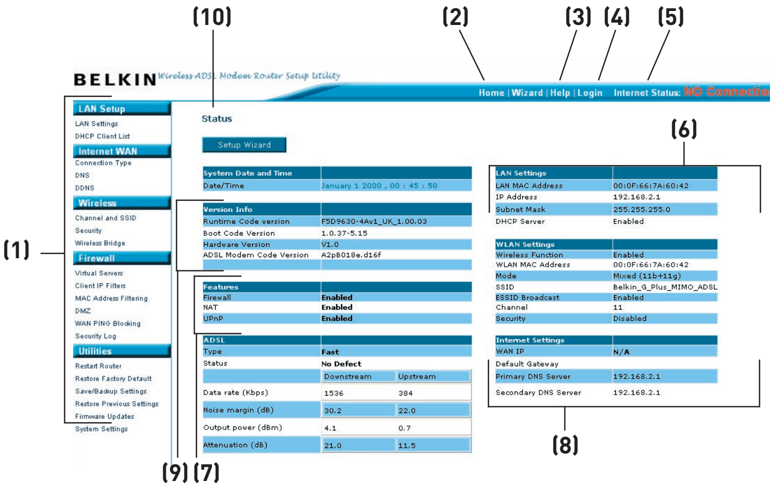
SSID	Belkin_G_Plus_MIMO_ADSL
Wireless Channel	11
Country	Other ISP
ISP	Other ISP
Connection Type	PPPoE
User Name	guest@Belkin.net
Password	password
VPI / VCI	0 / 38
Encapsulation	LLC
DNS	Auto
IP Address:	Automatically Assigned
NAT	Enabled
Firewall	Enabled
Service Name	
MTU	1492

Back Save/Reboot

Hinweis: Sie können den Konfigurationsassistenten jederzeit starten oder das links angezeigte Navigationsmenü verwenden, um Ihre Einstellungen zu ändern.

Übersicht über die Webgestützte Erweiterte Benutzeroberfläche

Sie gibt einen Überblick über den Status und die Einstellungen des Routers. Alle weiteren Konfigurationsseiten können von dieser Seite aus abgerufen werden.



1. **Navigationslinks**
   Wenn Sie auf einen dieser Links klicken, gelangen Sie direkt auf eine Einstellungsseite der Benutzeroberfläche. Die Links sind in mehrere Rubriken gegliedert und auf Registerkarten angeordnet, damit Sie die gesuchten Einstellungen leichter finden. Die Funktion der einzelnen Register wird angezeigt, wenn Sie auf den Titel der Registerkarten klicken.

2. **Schaltfläche „Home”**
   Die Schaltfläche „Home” finden Sie auf jeder Seite der Erweiterten Benutzeroberfläche. Mit ihr gelangen Sie zurück auf die Startseite.

3. **Schaltfläche „Hilfe”**
   Mit der Schaltfläche „Help” (Hilfe) öffnen Sie die Hilfeseiten des Routers. Die Hilfe kann auf vielen Seiten mit der Option „more info” (Weitere Informationen) aufgerufen werden, die neben vielen Abschnitten angezeigt wird.

4. **Schaltfläche „Anmelden/Abmelden”**
   Mit dieser Schaltfläche melden Sie sich am Router an oder ab. Wenn Sie am Router angemeldet sind, heißt die Schaltfläche „Logout” (Abmelden). Beim Anmelden gelangen Sie auf eine eigene Anmeldeseite, auf der Sie ein

Kennwort eingeben müssen. Wenn Sie sich am Router angemeldet haben, können Sie Änderungen an den Einstellungen vornehmen. Wenn Sie mit den Änderungen fertig sind, können Sie sich mit der Schaltfläche „Logout" (Abmelden) wieder vom Router abmelden. Weitere Hinweise zur Anmeldung finden Sie unter „Anmelden an den Router".

5. **Internet-Statusanzeige**

   Diese Anzeige steht auf allen Routerseiten zur Verfügung. Sie gibt den Verbindungsstatus des Routers an. Erscheint die grüne Anzeige „Connection OK" (Verbindung OK), ist der Router mit dem Internet verbunden. Besteht keine Verbindung zum Internet, meldet die Anzeige „no connection" (keine Verbindung) in roten Lettern. Die Anzeige wird automatisch aktualisiert, wenn Sie die Routereinstellungen ändern.

6. **LAN-Einstellungen**

   Ruft die LAN-seitigen Einstellungen des Routers ab. Änderungen an diesen Einstellungen können vorgenommen werden, indem Sie auf den Navigationslink „LAN" auf der linken Seite des Bildschirms klicken.

7. **Funktionen**

   Zeigt den Status von UPnP, NAT und Firewallfunktionen an. Sie können die Einstellungen ändern, indem Sie auf einen dieser Links oder auf einen der Navigationslinks links auf dem Bildschirm klicken.

8. **Internet-Einstellungen**

   Zeigt die Internet- und WAN-seitigen Einstellungen des mit dem Internet verbundenen Routers an. Änderungen an diesen Einstellungen können vorgenommen werden, indem Sie auf den Navigationslink „Internet/WAN" auf der linken Seite des Bildschirms klicken.

9. **Version**

   Ruft die Firmware-Version, Bootcode-Version, Hardwareversion und die Seriennummer des Routers ab.

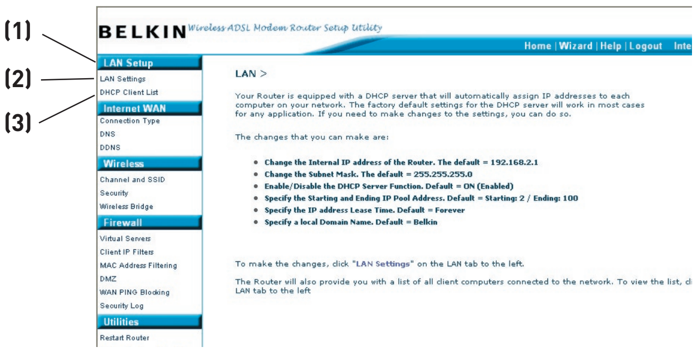
10. **Seitenname**

    Die Seite, auf der Sie sich befinden, ist durch diesen Namen gekennzeichnet. Er wird verwendet, wenn im Handbuch auf diese Seite verwiesen wird. Zum Beispiel verweist „LAN > LAN Settings" auf die Seite „LAN Settings" (LAN-Einstellungen).

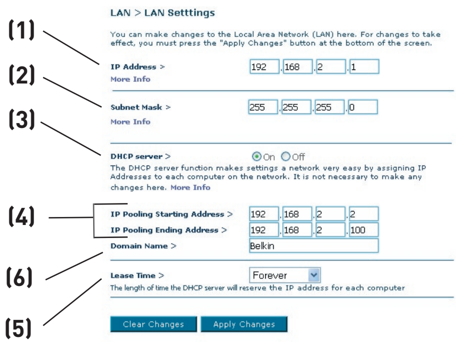
Ändern der LAN-Einstellungen

Hier können Sie alle Einstellungen für die interne LAN-Konfiguration des Routers überprüfen und ändern.

Durch Klicken auf den Reiter der Registerkarte „LAN" **(1)** öffnen Sie die Hauptseite der LAN-Einstellungen. Hier finden Sie eine kurze Beschreibung der Funktionen. Wenn Sie die Einstellungen überprüfen oder ändern möchten, klicken Sie auf „LAN Settings" (LAN-Einstellungen) **(2)** Mit „DHCP Client List" (DHCP-Client-Liste) rufen Sie die Liste der verbundenen Computer ab **(3)**.



LAN-Einstellungen



1. **IP-Adresse**

   Diese „IP-Adresse” ist die interne IP-Adresse des Routers. Die Standard-IP-Adresse ist 192.168.2.1. Um die Konfigurationsoberfläche zu öffnen, geben Sie diese IP-Adresse in die Adresszeile Ihres Browsers ein. Bei Bedarf können Sie die Adresse ändern. Geben Sie hierzu die neue IP-Adresse ein, und klicken Sie auf „Apply Changes” (Änderungen übernehmen). Achten Sie darauf, dass Sie eine nicht routbare IP-Adresse wählen. Beispiele für nicht routbare IP-Adressen:

   192.168.x.x (x steht für eine Zahl zwischen 0 und 255)

   10.x.x.x (x steht für eine Zahl zwischen 0 und 255)

2. **Subnet-Mask**

   Die Subnet-Mask braucht nicht verändert zu werden, da der Router die Länge automatisch an den IP-Adressentyp anpasst.

3. **DHCP-Server**

   Die DHCP-Serverfunktion erleichtert die Einrichtung eines Netzwerks, da jedem Computer automatisch eine IP-Adresse zugewiesen wird. Die Standardeinstellung ist „On” (aktiviert). Der DHCP-Server kann bei Bedarf deaktiviert werden; hierzu müssen Sie allerdings jedem Computer im Netzwerk eine statische IP-Adresse zuweisen. Um den DHCP-Server zu deaktivieren, wählen Sie „Off” (Aus), und klicken Sie auf „Apply Changes” (Änderungen übernehmen).

4. **IP-Pool**

   Der IP-Pool ist die Auswahl der IP-Adressen, die für eine dynamische Zuweisung an die Computer im Netzwerk reserviert sind. Die Vorgabe ist

2–100 (99 Computer). Wenn Sie diese Zahl ändern möchten, geben Sie eine neue Start- und eine neue Endadresse ein, und klicken Sie auf „Apply Changes” (Änderungen übernehmen). Der DCHP-Server kann 100 IP-Adressen automatisch zuweisen. Das heißt, dass der IP-Adressen-Pool, den Sie festlegen, höchstens 100 Computer umfasst. Wenn Sie zum Beispiel mit der Adresszahl 50 beginnen, muss die Endzahl kleiner oder gleich 150 sein, damit das Limit von 100 Clients nicht überschritten wird. Die Start-IP-Adresszahl muss kleiner sein als die Endzahl.

5. **Frist**

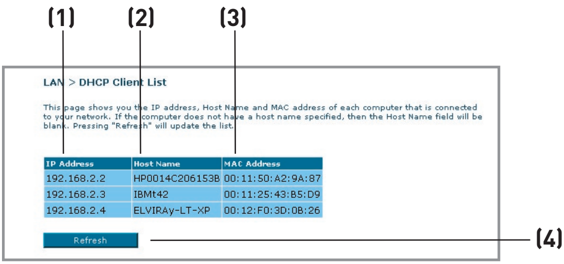
   Die Länge der Zeit, in der der DHCP-Server die IP-Adresse für jeden Computer reservieren wird. Es wird empfehlen, die Vorgabe „Forever” (Unbefristet) beizubehalten. Die Vorgabe bedeutet, dass sich die IP-Adresse eines Computers nicht mehr ändert, nachdem sie vom DHCP-Server zugewiesen wurde. Wenn Sie eine andere Frist einstellen, zum Beispiel einen Tag oder eine Stunde, wird die IP-Adresse nach dem Fristablauf freigegeben. Daher kann sich die IP-Adresse eines Computers im Laufe der Zeit ändern. Wenn Sie eine weiterführende Funktion des Routers wie DMZ oder Client-IP-Filter eingestellt haben, sind Sie an die IP-Adresse gebunden. Daher sollte die IP-Adresse beibehalten werden.

6. **Lokaler Domänenname**

   Die Werkseinstellung lautet „Belkin”. Sie können einen lokalen Domänennamen (Netzwerknamen) für Ihr Netzwerk festlegen. Diese Einstellung muss normalerweise nicht geändert werden, soweit Ihrerseits kein bestimmter Grund vorliegt. Sie können den Namen für Ihr Netzwerk frei wählen, z. B. „MY NETWORK” (MEIN NETZWERK).

DHCP-Client-Liste

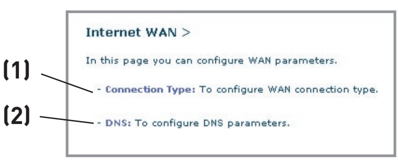
Sie können sich die Computer auflisten lassen, die mit dem Netzwerk verbunden sind (auch als Clients bezeichnet). Die Liste gibt die IP-Adresse der Computer an **(1)**, Ihre Hostnamen **(2)** (soweit zugewiesen) und die MAC-Adresse **(3)** ihrer Netzwerkadapter. Mit der Taste „Refresh” **(4)** (Aktualisieren) bringen Sie die Liste auf den neuesten Stand. Dadurch werden alle Änderungen sichtbar.



Internet/WAN

Auf der Registerkarte „Internet/WAN”, richten Sie den Router für die Verbindung mit Ihrem Internetanbieter ein. Der Router kann die Verbindung zu fast jedem ADSL-Anbietersystem herstellen, sofern Sie die Routereinstellungen an den Verbindungstyp anpassen. Die Verbindungseinstellungen werden Ihnen von Ihrem Internetprovider mitgeteilt. Um die vom Provider vorgeschriebenen Einstellungen am Router vorzunehmen, klicken Sie links auf dem Bildschirm auf „Connection Type” **(1)** (Verbindungstyp). Wählen Sie den verwendeten Verbindungstyp aus. Wenn Sie vom Anbieter DNS-Einstellungen erhalten haben, klicken Sie auf „DNS” **(2)**, um die DNS-Adressangaben für Provider einzugeben, die besondere Einstellungen verlangen.

Wenn Sie alle Einstellungen vorgenommen haben, meldet die Statusanzeige „Connection OK” (Verbindung ok), falls der Router korrekt konfiguriert wurde.



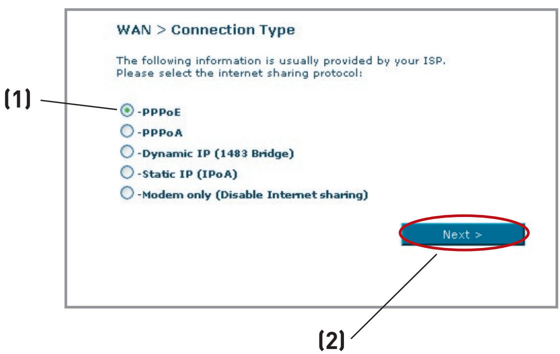
Verbindungstyp

Auf dieser Seite können Sie einen von fünf Verbindungstypen auswählen, je nach Angaben Ihres Internetproviders:

- PPPoE
- PPPoA
- Dynamic IP (1483 Bridged) (Dynamische IP [1483 Bridged])
- Static IP (IPOA) (Statische IP [IPOA])
- Modem Only (Disable Internet Sharing) (Nur Modem [Gemeinsame Internetnutzung wird deaktiviert])

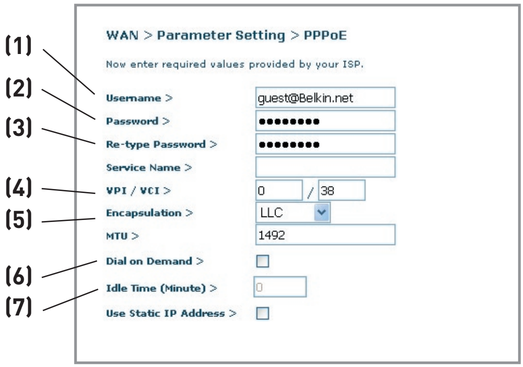
Hinweis: Beachten Sie den Anhang C in diesem Handbuch. Dort finden Sie einige gebräuchliche Parameter für die DSL-Interneteinstellungen. Wenn Sie sich der Einstellungen nicht sicher sind, wenden Sie sich bitte an Ihren Internetprovider.

Klicken Sie hierzu auf das entsprechende Optionsfeld **(1)** neben dem Verbindungstyp und dann auf „Next" (Weiter) **(2)**.



Einstellen des ISP-Verbindungstyps auf PPPoE oder PPPoA

PPPoE (Point-to-Point Protokoll über Ethernet) ist die Standardmethode, mit der Netzwerkgeräte miteinander verbunden werden. Sie benötigen einen Benutzernamen und ein Kennwort, um über das Netzwerk Ihres Internetanbieters auf das Internet zuzugreifen. PPPoA (PPP über ATM) ist dem PPPoE ähnlich, wird aber meist in Großbritannien verwendet. Wählen Sie „PPPoE" oder „PPPoA" aus und klicken Sie anschließend auf „Next" (Weiter). Geben Sie dann die Informationen von Ihrem Provider an und klicken Sie auf „Apply Changes" (Änderungen übernehmen), um die Einstellungen zu aktiveren.



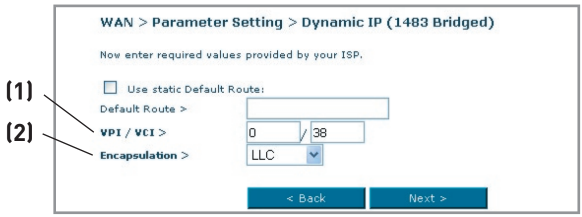
1. **Benutzername -** Geben Sie Ihren Benutzernamen ein. (Vom Internetprovider vergeben).
2. **Kennwort -** Geben Sie Ihr Kennwort ein. (Vom Internetprovider vergeben).
3. **Kennwort erneut eingeben -** Bestätigen Sie das Kennwort. (Vom Internetprovider vergeben).
4. **VPI/VCI -** Geben Sie Ihren Virtual Path Identifier (Virtuelle Pfaderkennung - VPI) und Virtual Circuit Identifier (Virtuelle Circuiterkennung - VCI) hier ein. (Vom Internetprovider vergeben).
5. **Kapselung -** Wählen Sie Ihre Kapselung aus (vom Internetprovider vergeben), um zu bestimmen, wie mit mehreren Protokollen bei ATM-Transportschicht (ATM transport layer) umgegangen wird.

   VC-MUX: PPPoA Virtual Circuit Multiplexer (Null-Kapselung) erlaubt es, pro virtuellem Circuit mit weniger Overheads nur ein Protokoll zugleich auszuführen.

   LLC: PPPoA Logical Link Control ermöglicht es, mehrere Protokolle mit einem virtuellen Circuit (mehr Overhead) zugleich auszuführen.
6. **Dial on Demand (Automatische DFÜ-Verbindung) -** Wenn Sie „Dial on Demand" wählen, wird Ihr Router automatisch mit dem Internet verbunden, wenn ein Benutzer einen Webbrowser öffnet.
7. **Zeitlimit (Minuten) -** Geben Sie das maximale Zeitlimit für die Internetverbindung an. Nach Ablauf dieser Zeit wird die Verbindung unterbrochen.

Einstellen Ihres Verbindungstyps auf Dynamische IP (1483 Bridged)

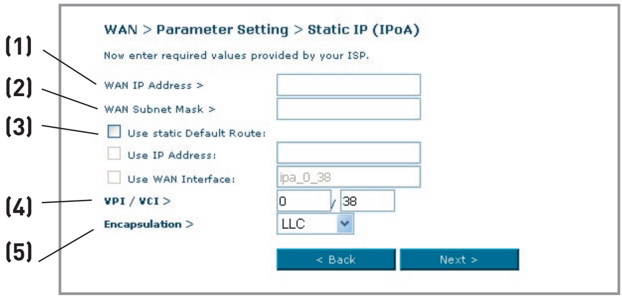
Diese Verbindungsmethode verbindet Ihr Netzwerk und das Netzwerk des Providers miteinander. Der Router erhält automatisch eine IP-Adresse vom DHCP-Server des Internetproviders (ISP).



1. **VPI/VCI -** Geben Sie Ihren Virtual Path Identifier (Virtuelle Pfaderkennung - VPI) und Virtual Circuit Identifier (Virtuelle Circuiterkennung - VCI) hier ein. Diese Erkennung wird vom Internetprovider erteilt.
2. **Kapselung -** Wählen Sie, ob Ihr Internetprovider LLC oder VC MUX verwendet.

Einstellen der ISP-Verbindung auf Statische IP (IPoA)

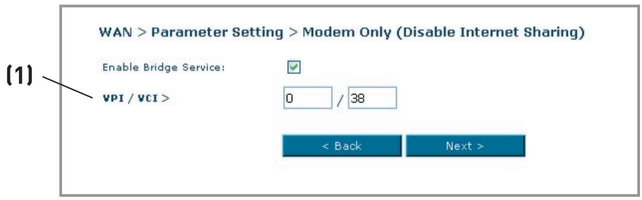
Dieser Verbindungstyp wird auch als „Classical IP over ATM” (Klassisches IP über ATM) oder „CLIP” bezeichnet, wobei der Internetprovider eine feste IP für Ihren Router erstellt.



1. **WAN-IP-Adresse –** Geben Sie eine IP-Adresse ein, die vom Internetprovider für die WAN-Schnittstelle des Routers erteilt wurde.
2. **WAN Subnet-Mask -** Geben Sie hier die Subnet-Mask ein, wie sie von Internetprovider erteilt wurde.
3. **Standardroute -** Geben Sie eine Standard-IP-Adresse ein. Wenn der Router die Zieladresse innerhalb des lokalen Netzwerks nicht finden kann, wird er die Pakete an die Standard-Gateway senden.
4. **VPI/VCI -** Geben Sie Ihren Virtual Path Identifier (Virtuelle Pfaderkennung - VPI) und Virtual Circuit Identifier (Virtuelle Circuiterkennung - VCI) hier ein. Diese Erkennung wird vom Internetprovider erteilt.
5. **Kapselung -** Wählen Sie, ob Ihr Internetprovider LLC oder VC MUX verwendet.

Einstellen Ihres Verbindungstyps auf „Nur Modem" (Gemeinsame Internetnutzung wird deaktiviert)

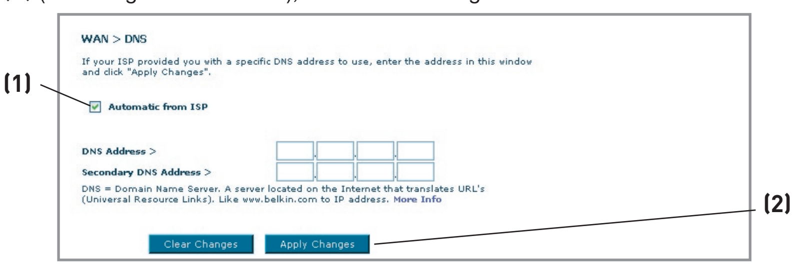
In diesem Modus funktioniert der Router einfach als Bridge zur Versendung von Paketen über den DSL-Anschluss. Dazu muss eine ergänzende Software auf dem Computer installiert werden, über die der Zugang zum Internet erfolgen soll.



1. **VPI/VCI -** Geben Sie Ihren Virtual Path Identifier (Virtuelle Pfaderkennung - VPI) und Virtual Circuit Identifier (Virtuelle Circuiterkennung - VCI) hier ein. (Vom Internetprovider vergeben).

DNS-Einstellungen (Domain Name Server - Domänennamenserver)

Als DNS (Domain Name Server) wird ein Server im Internet bezeichnet, der URLs (Universal Resource Links) wie „www.belkin.com" zu IP-Adressen auflöst. Bei vielen Providern ist eine Eingabe dieser Informationen in den Router unnötig. Wenn Ihnen der Provider keine bestimmte DNS-Adresse mitgeteilt hat, markieren Sie das Feld „Automatic from ISP" **(1)** (Automatisch vom ISP). Wenn Sie einen statischen Verbindungstyp verwenden, müssen Sie möglicherweise eine bestimmte DNS-Adresse sowie eine sekundäre DNS-Adresse angeben, damit die Verbindung ordnungsgemäß funktioniert. Wenn Sie mit einem dynamischen Verbindungstyp oder PPPoE arbeiten, müssen Sie wahrscheinlich keine DNS-Adresse eingeben. Lassen Sie dann das Kontrollkästchen „Automatic from ISP" (Automatisch vom ISP) markiert. Um die DNS-Adresseinstellungen einzugeben, deaktivieren Sie das Kontrollkästchen „Automatic from ISP", und geben Sie die DNS-Einträge in die entsprechenden Felder ein. Klicken Sie auf „Apply Changes" **(2)** (Änderungen übernehmen), um die Einstellungen zu sichern.



Verwenden der dynamischen DNS

Der dynamische DNS-Dienst ermöglicht es Ihnen, eine dynamische IP-Adresse in jeder der zahlreichen Domänen, die DynDNS.org anbietet, als statischen Hostnamen auszuweisen. Sie erlauben Ihren Netzwerkcomputern damit, leichter auf verschiedene Bereiche des Internets zuzugreifen. DynDNS.org bietet diesen Dienst für maximal fünf Hostnamen kostenlos im Internet an.

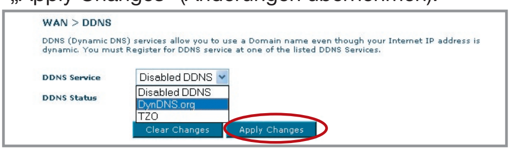
Der Dynamische DNSSM-Dienst ist ideal für private Internetseiten, Dateiserver oder um den Zugriff zu Ihrem Heim-PC von Ihrem Arbeitsplatz aus zu erleichtern. Verwenden Sie den Dienst, wenn Sie sicher gehen möchten, dass Ihr Hostname immer zu Ihrer IP-Adresse führt, unabhängig davon, wie oft diese von Ihrem Provider geändert wird. Auch wenn sich Ihre IP-Adresse ändert, können Ihre Freunde und Bekannte sie immer im Internet finden, indem Sie ersatzweise die Adresse ihrname.dyndns.org eingeben!

Um sich kostenlos für Dynamic DNS anzumelden, öffnen Sie die Seite http://www.dyndns.org.(englischsprachig).

Einstellen des Update-Clients für Dynamisches DNS

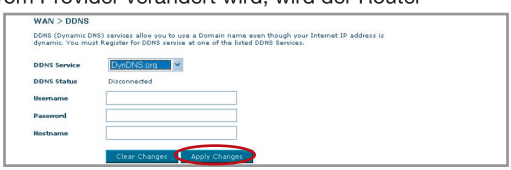
Sie müssen sich beim kostenlosen Aktualisierungsdienst von DynDNS.org anmelden, bevor Sie diese Funktion nutzen können. Nach der Registrierung befolgen Sie bitte diese Anweisungen.

1. Wählen Sie „DynDNS.org" aus der Dropdown-Liste aus. Klicken Sie auf „Apply Changes" (Änderungen übernehmen).



2. Geben Sie in das Feld „User Name" **(1) (Benutzername) Ihren DynDNS. org-Benutzernamen ein.** .
3. Geben Sie in das Feld „Password " (Kennwort) Ihr DynDNS.org-Kennwort ein **(2)**.
4. Geben Sie in das Feld „Domain Name" (Domänenname) den DynDNS.org-Domänennamen ein, den Sie mit DynDNS.org eingestellt haben, ein.**(3)**.
5. Klicken Sie auf „Apply Changes" (Änderungen übernehmen), um Ihre IP-Adresse zu aktualisieren.

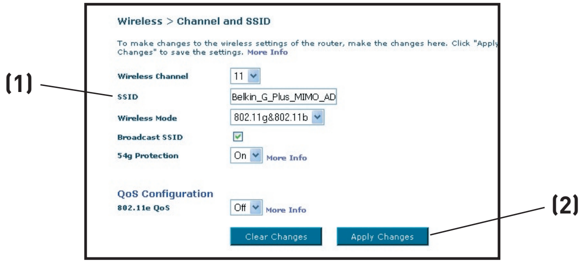
Immer wenn Ihre IP-Adresse vom Provider verändert wird, wird der Router automatisch die Server von DynDNS.org mit der neuen IP-Adresse aktualisieren. Sie können dies auch manuell tun, indem Sie auf die Schaltfläche „Apply changes"**(4) klicken**.



Funknetz

Auf der Registerkarte „Wireless” (Funknetz) können Sie die Einstellungen des kabellosen Netzwerks ändern. Sie können Änderungen am Namen des Funknetzwerks (SSID), am Betriebskanal und an der Sicherheitsverschlüsselung vornehmen.

Kanal und SSID



1. Wechseln des Funkkanals

Sie können einen von mehreren Betriebskanälen auswählen. In den USA stehen 11 Kanäle zur Auswahl, in Großbritannien und den meisten anderen europäischen Ländern 13 Kanäle. Bestimmte Länder haben abweichende Funkvorschriften. Der Router ist für den zulässigen Betrieb Ihres Landes konfiguriert. Der Standardkanal ist Kanal 11, es sei denn, Sie befinden sich einem Land, in dem Kanal 11 nicht zugelassen ist. Bei Bedarf können Sie den Kanal wechseln. Sind im Funkgebiet weitere kabellose Netzwerke in Betrieb, sollten Sie für Ihr Netzwerk einen Kanal wählen, der von diesen nicht genutzt wird. Wählen Sie am besten einen Kanal aus, der sich um mindestens fünf Kanalstufen von den anderen Netzwerken unterscheidet. Wenn zum Beispiel ein Netzwerk auf Kanal 11 betrieben wird, stellen Sie Ihr Netzwerk auf Kanal 6 oder einen niedrigeren Kanal ein. Sie wechseln den Kanal, indem Sie den Kanal aus der Dropdown-Liste wählen. Klicken Sie auf „Apply Changes” (Änderungen übernehmen). Die Änderung wird unmittelbar wirksam.

2. Ändern des Netzwerknamens (SSID)

Zur Kennzeichnung Ihres kabellosen Netzwerks dient die sogenannte SSID, der Netzwerkname. Die Standard-SSID des Routers ist „belkin54g”. Sie können sie beliebig verändern oder die Vorgabe beibehalten. Werden weitere kabellose Netzwerke im Funkbereich betrieben, sollten Sie eine eindeutige SSID festlegen, also eine SSID, die von keinem anderen Netzwerk in der Nähe genutzt wird. Sie können die SSID ändern, indem Sie die gewünschte SSID eingeben **(1)** und auf „Apply Changes” (Änderungen übernehmen) klicken**(2)**. Die Änderung wird unmittelbar wirksam. Wenn Sie die SSID ändern, müssen Ihre kabellos vernetzten Computer ggf. an den neuen Netzwerknamen angepasst werden. Informationen zur Vornahme dieser Änderung finden Sie in der Dokumentation Ihres Netzwerkadapters.

3. Verwenden der Funktion Broadcast ESSID (ESSID senden)

Aus Sicherheitsgründen können Sie festlegen, dass die SSID Ihres Netzwerks nicht gesendet wird. Danach wird Ihr Netzwerk so verborgen, dass es über die Standortübersicht von anderen Computern nicht erkannt wird. Wenn Sie das Senden der SSID ausschalten wollen, entfernen Sie die Markierung im Feld neben der Option „Broadcast SSID" (SSID rundsenden). Die Änderung wird unmittelbar wirksam. Jeder Computer muss jetzt genau auf die SSID Ihres Netzwerks eingestellt werden. Die SSID-Einstellung „ANY" (Beliebig) wird nicht mehr akzeptiert. Informationen zur Vornahme dieser Änderung finden Sie in der Dokumentation Ihres Netzwerkadapters.

Hinweis: Diese weiterführende Funktion sollte nur von erfahrenen Benutzern bedient werden.

4. Einstellen des Funkmodus

Ihr Router kann in zwei verschiedenen Funkmodi betrieben werden:

- **802.11b und 802.11g-** Wählen Sie diese Option, wenn Sie kabellose Clients mit den Standards 802.11b und 802.11g in Ihr Netzwerk einbinden wollen.
- **802.11g -** Verwenden Sie diesen Modus, wenn es in Ihrem Netzwerk keine 802.11b-Clients gibt. Mit dieser Option erzielen Sie die beste Leistung; 802.11b-Clients können jedoch nicht eingebunden werden.

5. Geschützter Modus

Als Teil der 802.11g-Spezifikation garantiert der geschützte Modus die Funktionalität mit 802.11g-Clients und -Access Points bei hohem 802.11b-Verkehr. Wenn der geschützte Modus aktiviert ist, sucht 802.11g nach anderen kabellosen Netzwerkaktivitäten, bevor Daten übertragen werden. Daher wird mit diesem Modus in Umgebungen mit hohem 802.11b-Datenverkehr oder -Interferenzen das beste Ergebnis erzielt. Wenn Sie in einer Umgebung mit sehr wenig oder keinem kabellosen Datenverkehr arbeiten, erreichen Sie die beste Leistung, wenn Sie den geschützten Modus deaktivieren.

Verschlüsselung/Sicherheit

Sicherung des Wi-Fi Netzwerks

Es folgen ein paar Möglichkeiten, mit denen Sie die Sicherheit Ihres kabellosen Netzwerks optimieren können und Ihre Daten vor unerwünschtem Zugriff schützen können. Dieses Kapitel richtet sich speziell an Benutzer, die Ihr Netzwerk privat oder in kleinen Unternehmen nutzen. Zum Zeitpunkt der Veröffentlichung gibt es vier Verschlüsselungsmethoden.

Name	64-Bit WEP (Wired Equivalent Privacy)	128-Bit WEP (Wired Equivalent Privacy)	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Akronym	64-Bit WEP	128-Bit WEP	WPA-TKIP/AES (oder nur WPA)	WPA2-AES (oder nur WPA2)
Sicherheit	Gut	Besser	Ausgezeichnet	Ausgezeichnet
Merkmale	Statische Schlüssel	Statische Schlüssel	Dynamische Schlüsselverschlüsselung und gegenseitige Authentifizierung	Dynamische Schlüsselverschlüsselung und gegenseitige Authentifizierung
	Verschlüsselung auf Basis von RC4 Algorithmus (normalerweise 40-Bit-Schlüssel)	Zusätzliche Sicherheit über 64-Bit WEP unter Benutzung einer Schlüssellänge von 104 Bits, ergänzt durch weitere 24 Bits Daten, die das System erzeugt	Zugefügtes TKIP (Temporal Key Integrity Protocol), damit Schlüssel rotieren und die Verschlüsselung verstärkt wird	AES (Advanced Encryption Standard) verursacht keinen Durchsatzverlust.

WEP (Wired Equivalent Privacy)

WEP ist ein verbreitetes Protokoll, das allen Wi-Fi-kompatiblen Geräten für kabellose Netzwerke Sicherheit verleiht. WEP schützt Daten in kabellosen Netzwerken auf einem Niveau, das mit verkabelten Netzwerken vergleichbar ist.

64-Bit WEP-Verschlüsselung

64-Bit WEP wurde mit 64-Bit-Verschlüsselung eingeführt, die aus einer Schlüssellänge von 40 Bits und 24 weiteren Bits an Daten, die vom System erzeugt werden, besteht (insgesamt 64 Bits). Manche Hardwarehersteller bezeichnen 64-Bit als 40-Bit-Verschlüsselung. Kurz nachdem die Technologie eingeführt worden war, haben Fachleute festgestellt, dass die 64-Bit-Verschlüsselung zu einfach zu entschlüsseln war.

128-Bit WEP-Verschlüsselung

Aufgrund der möglichen Sicherheitsschwächen von 64-Bit- WEP wurde eine sicherere Verschlüsselungsmethode, 128-Bit-WEP, entwickelt. 128-Bit-Verschlüsselung basiert auf einer Schlüssellänge von 104 Bits und 24 weiteren Bits, die durch das System erzeugt werden (insgesamt 128 Bits). Manche Hardwarehersteller bezeichnen 128-Bit als 104-Bit-Verschlüsselung.

Die meisten neueren Geräte für kabellose Netzwerke, die heutzutage auf dem Markt sind, unterstützen sowohl 64-Bit als auch 128-Bit WEP-Verschlüsselung. Vielleicht haben Sie aber ältere Geräte, die nur 64-Bit WEP unterstützen. Alle Belkin Produkte für kabellose Netzwerke unterstützen sowohl 64-Bit als auch 128-Bit WEP.

Verschlüsselungsschlüssel

Nachdem Sie sich entweder für den 64-Bit- oder den 128-Bit-WEP-Verschlüsselungsmodus entschieden haben, müssen Sie einen Schlüssel erzeugen. Wenn der Verschlüsselungsschlüssel nicht überall im kabellosen Netzwerk einheitlich ist, können Ihre Geräte für kabellose Netzwerke nicht miteinander kommunizieren. Auch kann keine Kommunikation mit anderen Netzwerken erfolgen.

Sie können Ihren Schlüssel eingeben, indem Sie den Hexadezimalschlüssel manuell eintragen oder Sie können eine Kennfolge im Feld „Passphrase" (Kennfolge) eintragen und „Generate" (Generieren) klicken, um einen Schlüssel zu erstellen. Ein Hexadezimalschlüssel ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0–9. Für 64-Bit-WEP müssen Sie 10 Hexadezimalzeichen eingeben. Für 128-Bit-WEP müssen Sie 26 Hexadezimalzeichen eingeben.

Die WEP-Kennfolge ist NICHT dasselbe wie ein WEP-Schlüssel. Ihre kabellose Netzwerkkarte benutzt diese Kennfolge, um Ihre WEP-Schlüssel zu bilden, aber andere Hardwarehersteller verwenden möglicherweise andere Erstellungsmethoden. Wenn Sie für Ihr Netzwerk Geräte von verschiedenen Herstellern benutzen, sollten Sie der Einfachheit halber den Hex-WEP-Schlüssel Ihres kabellosen Routers oder Access Points benutzen und ihn manuell in die Hex-WEP-Schlüssel Tabelle im Konfigurationsbildschirm Ihrer kabellosen Netzwerkkarte eingeben.

Verwenden eines Hexadezimalschlüssels

Ein Hexadezimalschlüssel ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0-9. 64-Bit-Schlüssel bestehen aus fünf zweistelligen Zahlen. 128-Bit-Schlüssel bestehen aus 13 zweistelligen Zeichen.

Beispiel:
AF 0F 4B C3 D4 = 64-Bit-Schlüssel
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-Bit-Schlüssel
Erstellen Sie in den Feldern unten Ihren Schlüssel, indem Sie in jedes Feld zwei Zeichen von A-F und 0-9 einfügen. Mit diesem Schlüssel programmieren Sie später die Verschlüsselungseinstellungen in Ihrem Router und den kabellosen Computern.

1 2 3 4 5 6 7 8 9 10 11 Kapitel

Hinweis an Mac-Benutzer: AirPort®-Produkte von Apple unterstützen in der Original-Ausführung nur Verschlüsselung mit 64 Bit. Apple AirPort 2-Produkte unterstützen sowohl 64-Bit- als auch 128-Bit-Verschlüsselung. Bitte prüfen Sie, welche Version Ihr Produkt nutzt. Wenn Sie Ihr Netzwerk nicht mit 128 Bit verschlüsseln können, sollten Sie es mit der 64-Bit-Verschlüsselung probieren.

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) ist ein neuer Wi-Fi-Standard, der über die Sicherheitsstandards von WEP hinausgeht. Wenn Sie WPA-Sicherheit nutzen wollen, müssen die Treiber und die Software Ihrer Geräte für kabellose Netzwerke entsprechend aufgerüstet sein. Die Aktualisierungen können Sie auf der Website Ihres Händlers finden. Es gibt zwei Arten von WPA-Sicherheitseinstellungen: WPA-Personal (PSK) und WPA-Enterprise (RADIUS).

WPA-Personal (PSK)

WPA-PSK verwendet einen sogenannten „Pre-shared Key (PSK)” als Sicherheitsschlüssel. Ein Netzwerk-Schlüssel ist ein Kennwort, das zwischen acht und 63 Zeichen lang ist. Es kann aus einer Kombination von Buchstaben, Ziffern oder anderen Zeichen bestehen. Jeder Client verwendet denselben Netzwerkschlüssel, um auf das Netzwerk zuzugreifen. Normalerweise ist dies der Modus, der in einem Heimnetzwerk verwendet wird.

WPA-Enterprise (RADIUS)

In diesem System verteilt der Radius-Server die Schlüssel automatisch an die Clients. Diese Technik wird häufig in Firmen eingesetzt. Eine Liste von Belkin-Produkten, die WPA unterstützen, finden Sie auf unserer Website unter**www.belkin.com/networking**.

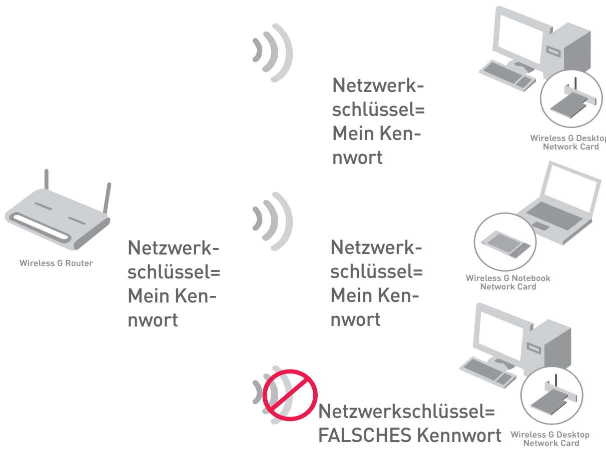
WPA2 (WiFi Protected Access)

WPA2 ist die zweite Generation des auf WPA basierenden 802.11i-Standards. Diese Methode bietet höhere Sicherheit im kabellosen Netzwerk, da eine komplexe Netzwerkauthentifizierung und eine stärkere AES-Verschlüsselungsmethode verwendet werden. Wie WPA gibt es WPA2 in zwei verschiedenen Modi: WPA2-Personal (PSK) und WPA2-Enterprise (RADIUS). Normalerweise ist WPA2-Personal (PSK) der Modus, der in einem Heimnetzwerk verwendet wird, während WPA-Enterprise (RADIUS) in Unternehmen verwendet wird, in denen der Netzwerkschlüssel von einem externen Radiusserver automatisch an die Clients verteilt wird.

Gemeinsame Nutzung von Netzwerkschlüsseln

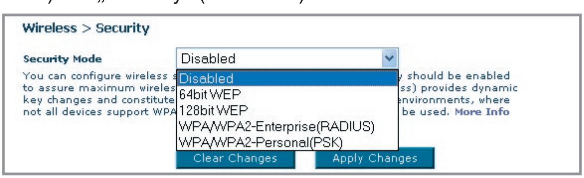
Die meisten Wi-Fi Produkte werden mit deaktivierter Sicherheitsfunktion geliefert. Sobald Ihr Netzwerk in Betrieb ist, müssen Sie WEP, WPA oder WPA2 aktivieren und sicherstellen, dass die Geräte ihres kabellosen Netzwerks denselben Netzwerkschlüssel verwenden.

Die kabellose G+ MIMO Deskop-Netzwerkkarte kann keinen Zugang zum Netzwerk bekommen, weil sie einen anderen Netzwerkschlüssel benutzt als den, der auf ihrem kabellosen G+ MIMO Router konfiguriert ist.



Änderungen der Sicherheitseinstellungen des Funknetzwerks

Ihr Router ist mit WPA/WPA2 (Wi-Fi Protected Access) ausgestattet - dem neuesten Sicherheitsstandard für kabellose Netzwerke. Er unterstützt auch den alten Sicherheitsstandard WEP (Wired Equivalent Privacy). Werkseitig ist die Sicherheitsfunktion deaktiviert. Um diese zu aktivieren, müssen Sie zuerst festlegen, welchen Standard Sie verwenden möchten. Um die Sicherheitseinstellungen zu bearbeiten, klicken Sie auf der Registerkarte „Wireless” (Funknetz) auf „Security” (Sicherheit).



1 2 3 4 5 6 7 8 9 10 11 Kapitel

WEP-Einstellung

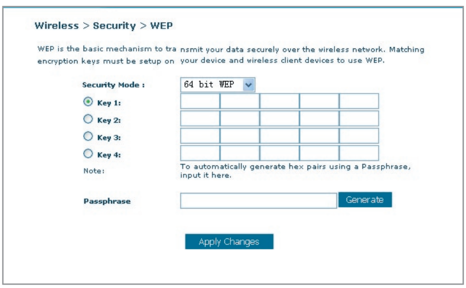
64-Bit-WEP-Verschlüsselung

1. Wählen Sie im Dropdown-Menü die Option „64-bit WEP".
2. Nachdem Sie den WEP-Verschlüsselungsmodus gewählt haben, können Sie den Schlüssel eingeben, indem Sie den Hexadezimalschlüssel manuell eintragen.

Ein Hexadezimalschlüssel ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0–9. Für 64-Bit-WEP müssen Sie 10 Hexadezimalzeichen eingeben.

Beispiel:

AF 0F 4B C3 D4 = 64-Bit-WEP-Schlüssel



3. Klicken Sie auf „Apply Changes" (Änderungen übernehmen), um abzuschließen. Jetzt ist die Verschlüsselung im Router eingestellt. Jeder Computer in Ihrem kabellosen Netzwerk muss jetzt mit denselben Sicherheitseinstellungen konfiguriert werden.

ACHTUNG: Wenn Sie für die Einstellung des kabellosen Routers oder Access Points einen Computer mit kabellosem Client verwenden, müssen Sie die Sicherheitsfunktion für diesen kabellosen Client aktivieren, damit Sie die Verbindung nicht unterbrochen wird. Notieren Sie sich Ihren Schlüssel, bevor Sie Änderungen vornehmen

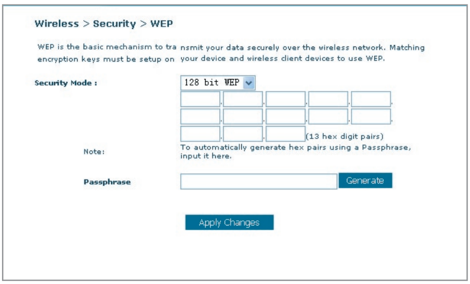
128-Bit-WEP-Verschlüsselung

1. Wählen Sie im Dropdown-Menü die Option „128-bit WEP”.
2. Nachdem Sie den WEP-Verschlüsselungsmodus gewählt haben, können Sie den Schlüssel eingeben, indem Sie den Hexadezimalschlüssel manuell eintragen.

   Ein Hexadezimalschlüssel ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0–9. Für 128-Bit-WEP müssen Sie 26 Hexadezimalzeichen eingeben.

   Beispiel:

   C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-Bit-WEP-Schlüssel



3. Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um abzuschließen. Jetzt ist die Verschlüsselung im Router eingestellt. Jeder Computer in Ihrem kabellosen Netzwerk muss jetzt mit denselben Sicherheitseinstellungen konfiguriert werden.

ACHTUNG: Wenn Sie für die Einstellung des kabellosen Routers oder Access Points einen Computer mit kabellosem Client verwenden, müssen Sie die Sicherheitsfunktion für diesen kabellosen Client aktivieren, damit Sie die Verbindung nicht unterbrochen wird. Notieren Sie sich Ihren Schlüssel, bevor Sie Änderungen vornehmen

WPA-Einstellung

Hinweis: Um WPA zu verwenden, müssen alle Ihre Clients auf die Software und Treiber, die WPA unterstützen, aktualisiert sein. Zum Zeitpunkt der Erstellung dieses Benutzerhandbuchs ist von Microsoft ein kostenloses Sicherheitspatch als Download erhältlich. Dieses Patch gilt nur für das Betriebssystem Windows XP. Sie benötigen auch die aktuellen Treiber von Belkin für Ihre kabellose Notebook-

Netzwerkkarte (Wireless G). Diese finden Sie auf der Support-Website von Belkin. Andere Betriebssysteme können zur Zeit nicht unterstützt werden. Das Patch von Microsoft unterstützt nur Geräte mit WPA-aktivierten Treibern, wie die 802.11g-Produkte von Belkin.

Es gibt zwei Arten von WPA-Sicherheitseinstellungen: WPA-Personal (PSK) und WPA-Enterprise (RADIUS). WPA-Personal (PSK) verwendet sogenannte pre-shared Schlüssel zur Sicherheitskodierung. Ein Pre-Shared Schlüssel ist ein Kennwort, das zwischen acht und 63 Zeichen lang ist. Es kann aus einer Kombination aus Buchstaben, Zahlen und anderen Zeichen bestehen. Jeder Client verwendet denselben Schlüssel, um auf das Netzwerk zuzugreifen. Normalerweise ist dies der Modus, der in einem Netzwerk zu Hause verwendet wird.

WPA-Enterprise (RADIUS) ist ein System, in dem ein Radius-Server die Schlüssel an die Clients automatisch verteilt. Diese Technik wird typischerweise in einer Unternehmensumgebung eingesetzt.

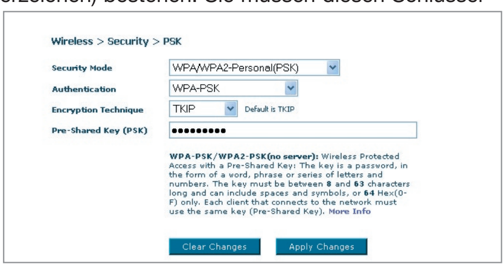
WPA-Personal einstellen (PSK)

1. Wählen Sie im Dropdown-Menü „Security Mode” (Sicherheitsmodus) „WPA/WPA2-PSK” aus.

2. Wählen Sie „WPA-PSK” zur Authentifizierung aus.

3. Wählen Sie als Verschlüsselungstechnik „TKIP” aus. Diese Einstellungen müssen mit denen Ihrer Clients übereinstimmen.

4. Geben Sie Ihren Pre-Shared Key ein. Er kann aus acht bis 63 Zeichen (Buchstaben, Ziffern, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten. Ihr PSK kann zum Beispiel heißen: „Familie Manns Netzwerkschlüssel”.

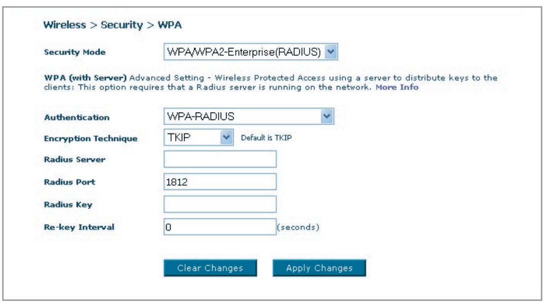


5. Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.

WPA-Enterprise (RADIUS) einstellen

Wenn Sie in Ihrem Netzwerk einen Radius-Server verwenden, um die Schlüssel an die Clients zu verteilen, verwenden Sie diese Einstellung.

1. Wählen Sie im Dropdown-Menü „Security Mode” (Sicherheitsmodus) „WPA/WPA2—Enterprise (RADIUS)” aus.
2. Wählen Sie „WPA-RADIUS” zur Authentifizierung
3. Wählen Sie als Verschlüsselungstechnik „TKIP” aus. Diese Einstellungen müssen identisch mit denen Ihrer Clients sein
4. Geben Sie die IP-Adresse des Radius-Servers in die Felder unter „Radius Server” ein.
5. Geben Sie den Radius-Schlüssel in das Feld „Radius Key” (Radius-Schlüssel) ein.
6. Geben Sie das Schlüsselintervall ein. Das Schlüsselintervall gibt an, wie oft die Schlüssel verteilt werden (in Paketen).
7. Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.



WPA2-Anforderungen

WICHTIG: Wenn Sie die WPA2-Sicherheitsfunktion verwenden wollen, müssen alle verwendeten Computer und Adapter kabelloser Clients mit aktualisierten Patches, Treibern und aktualisierter Software des Client-Dienstprogramms ausgestattet sein, die WPA2 unterstützen. Zum Zeitpunkt der Erstellung dieses Benutzerhandbuchs sind kostenlose Sicherheitspatches von Microsoft als Download erhältlich. Diese Patches gelten nur für das Betriebssystem Windows XP. Andere Betriebssysteme können zur Zeit nicht unterstützt werden.

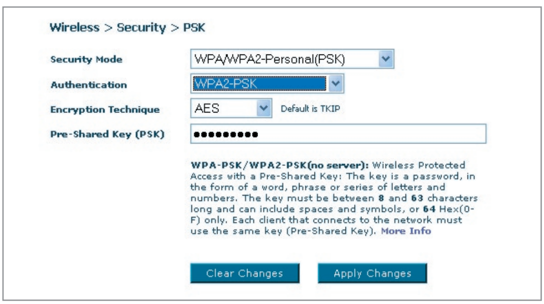
Für Windows XP Computer, die nicht mit Service Pack 2 (SP2) ausgestattet sind, ist eine Datei von Microsoft mit dem Namen „Windows XP Support Patch for Wireless Protected Access (KB 826942)” als kostenloser Download erhältlich. Sie finden Sie unter: http://support.microsoft.com/?kbid=826942.

Für Windows XP mit Service Pack 2 stellt Microsoft einen kostenlosen Download zur Verfügung, mit welchem Sie die Komponenten der kabellosen Clients so aktualisieren können, dass Sie WPA2 (KB893357) unterstützen. Die Aktualisierung steht Ihnen unter folgender Adresse zur Verfügung: http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

WICHTIG: All Ihre Netzwerkkarten/Adapter kabelloser Clients müssen WPA2 unterstützen und entsprechend über die neuesten Treiber verfügen. Aktualisierungen der meisten kabellosen Netzwerkkarten von Belkin finden Sie auf der Support Site von Belkin: www.belkin.com/networking

WPA2-Personal einstellen (PSK)

1. Wählen Sie im Dropdown-Menü „Security Mode" (Sicherheitsmodus) „WPA/WPA2-PSK (PSK)" aus.
2. Wählen Sie „WPA2-Personal (PSK)" zur Authentifizierung.
3. Wählen Sie als Verschlüsselungstechnik „AES" aus. Diese Einstellungen müssen mit denen Ihrer Clients übereinstimmen.
4. Geben Sie Ihren Pre-Shared Key (PSK) ein. Er kann aus acht bis 63 Zeichen (Buchstaben, Ziffern, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten. Ihr PSK kann zum Beispiel heißen: „Familie Manns Netzwerkschlüssel".



5. Klicken Sie auf „Apply Changes" (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.

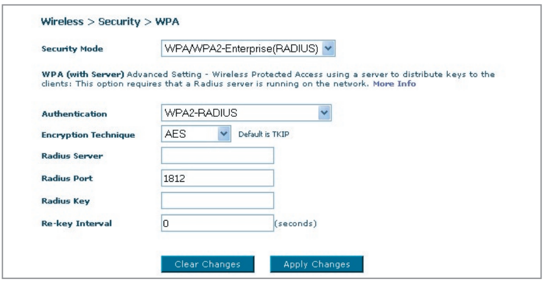
WPA2-Enterprise (RADIUS) einstellen

Wenn Sie in Ihrem Netzwerk einen Radius-Server verwenden, um die Schlüssel an die Clients zu verteilen,

verwenden Sie diese Einstellung.

1. Wählen Sie im Dropdown-Menü „Security Mode" (Sicherheitsmodus) „WPA/WPA2—Enterprise (RADIUS)" aus.
2. Wählen Sie „WPA2-RADIUS" zur Authentifizierung
3. Wählen Sie als Verschlüsselungstechnik „AES" aus. Diese Einstellungen müssen identisch mit denen Ihrer Clients sein

4. Geben Sie die IP-Adresse des Radius-Servers in die Felder unter „Radius Server” ein.
5. Geben Sie den Radius-Schlüssel in das Feld „Radius Key” (Radius-Schlüssel) ein.
6. Geben Sie das Schlüsselintervall ein. Das Schlüsselintervall gibt an, wie oft die Schlüssel verteilt werden (in Paketen).
7. Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.



WICHTIG: Stellen Sie sicher, dass die Computer Ihres kabellosen Netzwerks über die Aktualisierungen verfügen, die für die Verwendung von WPA2 erforderlich sind, und dass die Einstellungen eine korrekte Verbindung mit dem Router zulassen.

Einstellung der Sicherheitsfunktion des Netzwerk-Adapters

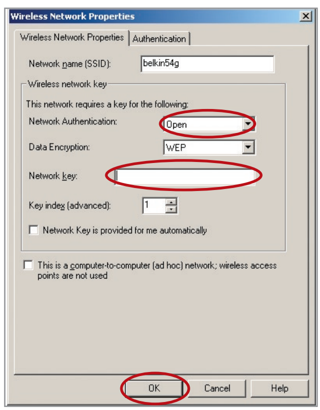
Hinweis: In diesem Abschnitt finden Sie Informationen zum Einstellen der Sicherheitsfunktion Ihres Netzwerk-Adapters. An dieser Stelle sollten Sie Ihren kabellosen Router oder Access Point bereits auf die Verwendung von WPA2, WPA oder WEP eingestellt haben. Für eine kabellose Verbindung müssen Sie Ihre kabellose Notebook- oder Desktop-Karte auf die gleiche Sicherheitsstufe einstellen.

Belkin G+ MIMO Netzwerkkarten verfügen über ein benutzerfreundliches Dienstprogramm für kabellose Netzwerke. Klicken Sie auf der Liste mit verfügbaren Netzwerken einfach auf den Namen Ihres kabellosen Netzwerks (SSID) und geben Sie Ihren Pre-Shared Key (PSK) ein. Mehr Informationen hierzu finden Sie im Benutzerhandbuch Ihrer kabellosen Netzwerkkarte von Belkin.

Die meisten Computer lassen sich auch über das Fenster „Eigenschaften von Drahtlose Netzwerkverbindung” unter Microsoft Windows für den Router einrichten. Es folgen zwei Beispiele:

Verbinden Ihres Computers mit einem kabellosen Netzwerk, das einen 64-Bit- oder 128-Bit WEP-Schlüssel erfordert

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network” (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen. Mit der Schaltfläche „Advanced” (Weitere Optionen) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
2. Wählen Sie auf der Registerkarte „Wireless Network Properties” (Netzwerkeigenschaften) einen Netzwerknamen aus der Liste „Available networks” (Verfügbare Netzwerke) aus und klicken Sie auf „Properties” (Eigenschaften).
3. Wählen Sie bei „Data Encryption” (Datenverschlüsselung) „WEP”.
4. Das untere Feld „Network key is provided for me automatically” (Netzwerkschlüssel wird automatisch vergeben) darf nicht aktiviert sein. Wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk herzustellen, wenden Sie sich bitte an Ihren Netzwerkadministrator für den Fall, dass dieses Feld aktiviert werden muss.
5. Geben Sie Ihren WEP-Schlüssel in das Feld „Network Key” (Netzwerkschlüssel) ein.

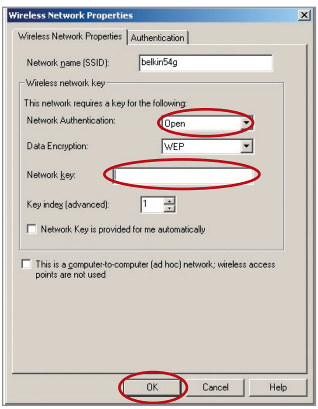


Wichtig: Ein WEP-Schlüssel ist eine Kombination aus Zahlen und Buchstaben von A-F und 0-9. Für 128-Bit WEP müssen Sie 26 Zeichen eingeben. Für 64-Bit-WEP müssen Sie zehn Zeichen eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres kabellosen Routers oder Access Points übereinstimmen.

6. Klicken Sie auf „OK”, um die Einstellungen zu speichern.

Verbinden Ihres Computers mit einem kabellosen Netzwerk, das einen WEP-PSK (kein Server) erfordert.

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network” (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen. Mit der Schaltfläche „Advanced” (Weitere Optionen) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
2. Wählen Sie auf der Registerkarte „Wireless Network” (Kabelloses Netzwerk) einen Netzwerknamen aus der Liste „Available networks” (Verfügbare Netzwerke) aus und klicken Sie auf „Configure” (Konfigurieren).
3. Wählen Sie unter „Network Authentication” (Netzwerk-Authentifizierung) den Eintrag „WPA-PSK (No Server)” (WPA-PSK [Kein Server] aus.
4. Geben Sie Ihren WEP-Schlüssel in das Feld „Network Key” (Netzwerkschlüssel) ein.

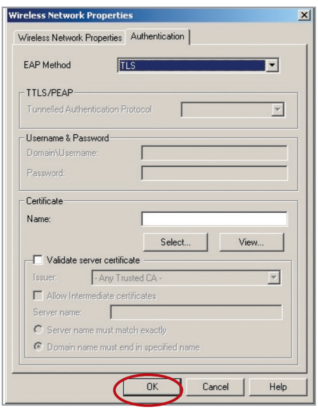


Wichtig: Ein WPA-PSK ist eine Kombination aus Zahlen und Buchstaben von A-Z und 0-9. Für WPA-PSK können Sie acht bis 63 Zeichen eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres kabellosen Routers oder Access Points übereinstimmen.

5. Klicken Sie auf „OK”, um die Einstellungen zu speichern.

Verbinden Sie Ihren Computer mit einem kabellosen Netzwerk, das WPA (mit Radius-Server) erfordert.

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network” (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen. Mit der Schaltfläche „Advanced” (Weitere Optionen) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
2. Wählen Sie auf der Registerkarte „Wireless Network” (Kabelloses Netzwerk) einen Netzwerknamen aus der Liste „Available networks” (Verfügbare Netzwerke) aus und klicken Sie auf „Configure” (Konfigurieren).
3. Wählen Sie unter „Network Authentication” (Netzwerk-Authentifizierung) den Eintrag „WPA” aus.
4. Wählen Sie auf der Registerkarte „Authentication” (Authentifizierung) die Einstellungen, die Ihnen von Ihrem Netzwerkadministrator angegeben werden.



5. Klicken Sie auf „OK”, um die Einstellungen zu speichern.

WPA/WPA2 für kabellose Desktop- und Notebookkarten von Drittanbietern einstellen

Für kabellose Desktop- und Notebookkarten von Drittanbietern, die nicht mit WPA/WPA2-Software ausgestattet sind, kann ein Sicherheitspatch von Microsoft mit dem Namen „Windows XP Support Patch for Wireless Protected Access” kostenlos heruntergeladen werden.

Manuelle Konfiguration des Routers

Hinweis: Dieses von Microsoft zur Verfügung gestellte Patch gilt nur für das Betriebssystem Windows XP. Andere Betriebssysteme können zur Zeit nicht unterstützt werden.

Wichtig: Sie müssen auch überprüfen, ob der Hersteller der kabellosen Karte WPA/WPA2 unterstützt und Sie die aktuellsten Treiber heruntergeladen und installiert haben.

Unterstützte Betriebssysteme:

- **Windows XP Professional**
- **Windows XP Home Edition**

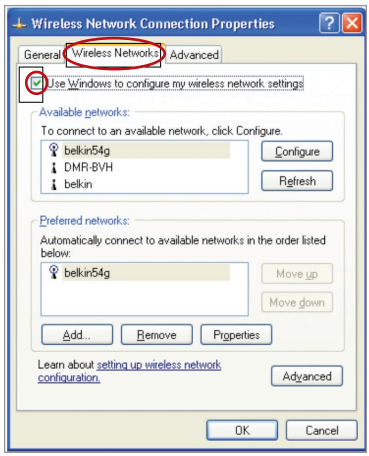
Windows XP Wireless Network Utility (Dienstprogramm für kabellose Netzwerke) für WPA/WPA2-PSK einstellen

Um WPA-PSK einsetzen zu können, müssen Sie das Windows Wireless Network Utility (Kabelloses Netzwerkprogramm) verwenden. Gehen Sie dazu folgendermaßen vor:

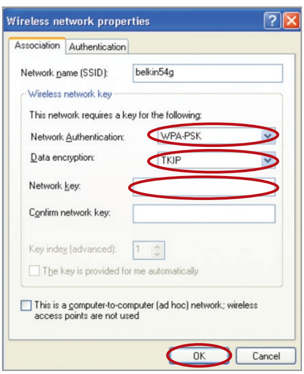
1. Klicken Sie unter Windows XP auf „Start > Systemsteuerung > Netzwerkverbindungen".

2. Klicken Sie mit der rechten Maustaste auf „Drahtlose Netzwerkverbindung" (Wireless Network Connection) und wählen Sie „Eigenschaften".

3. Klicken Sie mit der rechten Maustaste auf „Drahtlose Netzwerke" (Wireless Networks). Das folgende Fenster wird angezeigt. Vergewissern Sie sich, dass das Kontrollkästchen „Use Windows to configure my wireless network settings" (Windows zum Konfigurieren der Einstellungen verwenden) markiert ist.



4. Klicken Sie auf die Registerkarte „Drahtlose Netzwerke", dann auf die Schaltfläche „Konfigurieren". Das folgende Fenster wird angezeigt.



Hinweis: Wählen Sie „WPA" aus, wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk herzustellen, in welchem ein Authentifizierungs server, z.B. ein Radius-Server, verwendet wird. Wenden Sie sich für weitere Informationen bitte an Ihren Netzwerkadministrator.

5. Nutzer von Heim- oder kleinen Unternehmensnetzwerken wählen bei „Network Authentication" (Netzwerk-Authentifizierung) „WPA-PSK" oder „WPA2-PSK".

6. Wählen Sie unter „Data Encryption” (Datenverschlüsselung) „TKIP” oder „AES”. Diese Einstellung muss identisch mit der des Routers sein.

7. Geben Sie Ihren Schlüssel in das Feld „Network Key” (Netzwerkschlüssel) ein.

Wichtiger Hinweis: Geben Sie Ihren Pre-Shared Key (PSK) ein. Er kann aus acht bis 63 Zeichen (Buchstaben, Ziffern, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten.

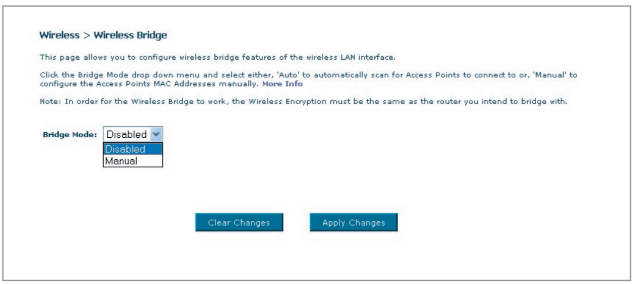
8. Klicken Sie auf „OK”, um die Einstellungen zu übernehmen.

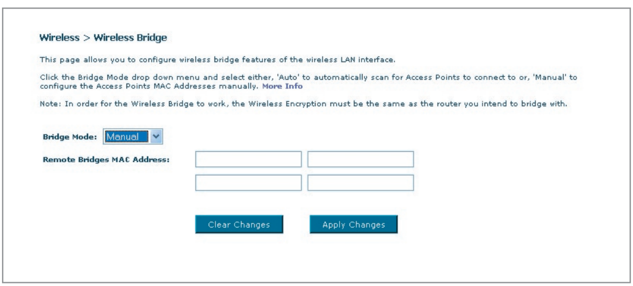
Wireless Bridge (Funkbrücke)

Die Funkbrücke (WDS-System) verbindet kabellose Router und Access Points zur Erweiterung eines Netzwerks.

Klicken auf das Dropdown-Menü neben „Bridge Mode” (Bridge-Modus), um auszuwählen zwischen:

Disabled (Deaktiviert): Deaktivierung der Funkbrücke (Vorgabe)





Manual (Manuell): Manuelle Eingabe von MAC-Adressen von Access Points, mit denen Sie eine Verbindung herstellen wollen.

1 Funkkanäle von Router und Access Point müssen übereinstimmen.

2 Sicherheitseinstellungen (WEP) von Router und Access Point müssen übereinstimmen.

3 Wenn der MAC-Filter aktiviert ist, muss der Benutzer die WLAN MAC-Adresse(n) des Routers/Access Points ergänzen, damit Kommunikation zwischen diesen Geräten stattfinden kann.

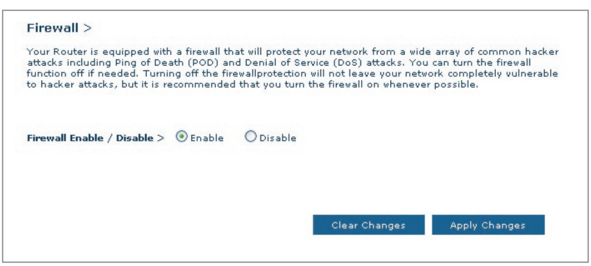
4 Wenn ein durch WPA geschütztes Netzwerk verwendet wird, muss die SSID beider Access Points genau übereinstimmen.

Firewall

Ihr Router verfügt über eine Firewall, die Ihr Netzwerk vor zahlreichen Hacker-Angriffen schützt:

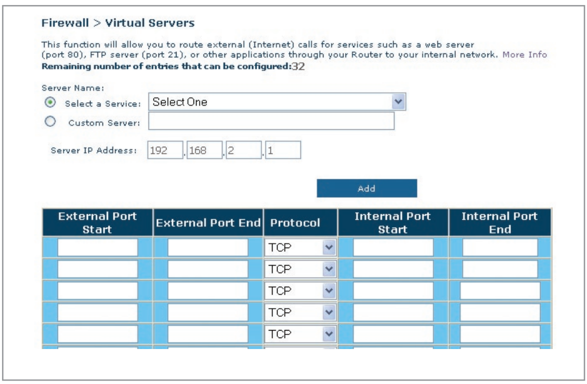
- IP-Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP mit Nullänge
- Smurf Attack
- TCP Null Scan
- SYN Flood
- UDP Flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment-Flooding

Außerdem verdeckt die Firewall Ports, die oft zu Angriffen auf Netzwerke missbraucht werden. Diese Ports werden so abgeschirmt, dass sie für potentielle Hacker nicht sichtbar sind. Sie können die Firewall-Funktion bei Bedarf deaktivieren. Es wird jedoch empfohlen, die Firewall aktiv zu lassen. Wenn Sie den Firewall-Schutz deaktivieren, ist Ihr Netzwerk Angriffen nicht völlig schutzlos ausgeliefert; die Gefahr unbefugter Eingriffe wächst jedoch.



Virtuelle Server

Mit der Funktion „Virtual Servers” (Virtuelle Server) können Sie externe Anrufe (aus dem Internet) von Diensten wie Webserver (Port 80), FTP-Server (Port 21) oder anderen Anwendungen über Ihren Router in Ihr internes Netzwerk umleiten. Da Ihre internen Computer durch eine Firewall geschützt sind, kann auf diese aus dem Internet nicht zugegriffen werden, weil sie dort nicht „sichtbar” sind. Wenn Sie die virtuelle Serverfunktion für eine bestimmte Anwendung einstellen müssen, sollten Sie Kontakt zum Hersteller des Programms aufnehmen, um dort zu erfahren, welche Port-Einstellungen Sie vornehmen müssen. Sie können die Port-Informationen manuell in den Router eingeben.



Auswählen einer Anwendung

Aus einer Liste können Sie gängige Anwendungen auswählen. Klicken Sie auf „Select a Service” (Service wählen) und wählen Sie dann Ihre Anwendung aus der Drop-Down-Liste. Die Einstellungen werden in die angegebene Zeile übertragen. Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um die Einstellungen für diese Anwendung zu sichern.

Manuelle Eingabe von Einstellungen in den virtuellen Server

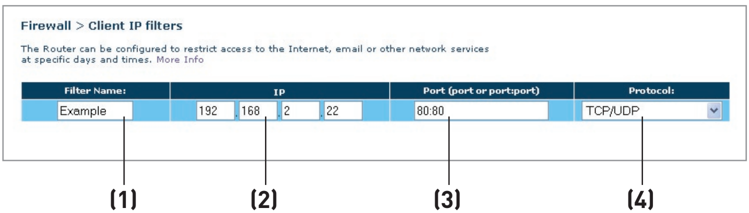
Klicken Sie zur manuellen Eingabe der Einstellungen auf „Custom Server” (Benutzerdefinierter Server) und geben Sie den Namen Ihres Servers ein. Geben Sie die IP-Adresse des Servers in das Feld für den internen Computer ein und dann die/den Port(s), die freigegeben werden müssen. Wählen Sie dann den Protokolltyp (TCP oder UDP) und klicken Sie auf „Add” (Hinzufügen).

Das Öffnen von Ports in Ihrer Firewall kann ein Sicherheitsrisiko darstellen. Das Aktivieren und Deaktivieren von Einstellungen geht schnell von der Hand.

Daher sollten Sie die Einstellungen deaktivieren, wenn Sie eine bestimmte Anwendung momentan nicht verwenden.

Client-IP-Filter

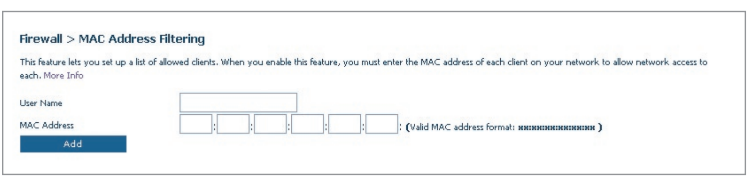
Sie können den Router so einstellen, dass der Zugriff auf das Internet, E-Mail oder andere Netzwerke auf bestimmte Tage und Zeiten beschränkt wird.



Wenn Sie z. B. den Internet-Zugriff für einen bestimmten Computer einschränken möchten, geben Sie den Namen des Filters im Feld „Filter Name” ein **(1)** und geben Sie seine IP-Adresse in das IP-Feld ein **(2)**. Geben Sie dann „80:80” in das Port-Feld**(3)** ein. Wählen sie dann im Drop-Down-Menü
„Protocol” (Protokoll) aus **(4)**. Klicken Sie auf „Apply Changes” (Änderungen übernehmen). Dem Computer mit der angegebenen IP-Adresse wird jetzt der Internet-Zugriff verweigert.

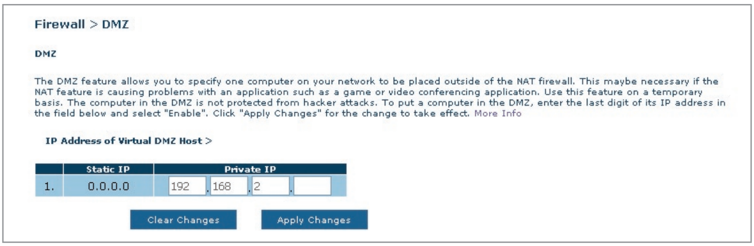
MAC Adress-Filter

Der MAC-Adressfilter ist eine leistungsstarke Sicherheitsfunktion, mit der Sie festlegen können, welche Computer für das Netzwerk zugelassen sind. Computern, die nicht in der Filterliste verzeichnet sind, wird der Zugriff auf das Netzwerk verweigert. Wenn Sie diese Funktion aktivieren, müssen Sie einen Namen für den Benutzer und die MAC-Adressen aller Clients in Ihrem Netzwerk eintragen, damit sie auf das Netzwerk zugreifen können. Klicken Sie dann auf „Add” (Hinzufügen), um die Einstellungen zu speichern.



DMZ (Demilitarized Zone: Demilitarisierte Zone)

Wenn Sie einen Client-PC haben, auf dem hinter der Firewall keine Internetanwendung richtig ausgeführt werden kann, können Sie den Client für ungehinderten Internetzugriff einstellen. Das kann erforderlich sein, wenn die NAT-Funktion bei einer Anwendung Probleme verursacht, zum Beispiel bei einem Spiel oder einer Videokonferenzanwendung. Verwenden Sie diese Funktion nur zeitweise. **Der DMZ-Computer ist NICHT vor Hacker-Angriffen geschützt.**

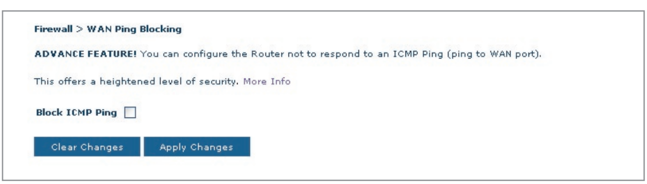


Um einen Computer in die DMZ zu versetzen, geben Sie die LAN-IP-Adresse in das Feld für die „Private IP" (Private IP-Adresse) ein und klicken Sie auf „Apply Changes" (Änderungen übernehmen), um die Änderungen zu aktivieren.

Blockieren von ICMP-Pings

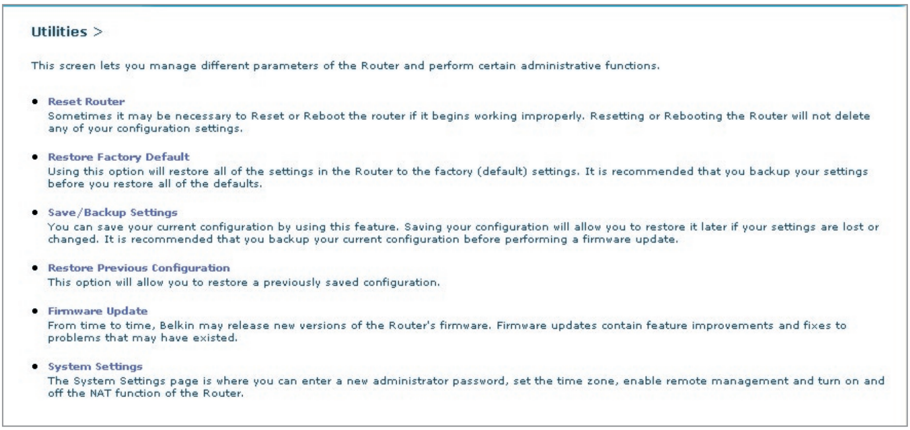
Computerhacker bedienen sich sogenannter Pings, um potenzielle Opfer im Internet zu finden. Über die Ping-Prüfung einer IP-Adresse und die Antwort des adressierten Rechners kann ein Hacker Angriffspunkte feststellen. Der Router kann so eingerichtet werden, dass er auf ICMP-Pings von außen nicht antwortet. Dadurch verbessern Sie den Schutz Ihres Routers.

Um die Ping-Antwort zu deaktivieren, wählen Sie „Block ICMP Ping" **(1)** und klicken auf „Apply Changes" (Änderungen übernehmen). Der Router lässt jetzt ICMP-Pings unbeantwortet.



Dienstprogramme

Auf der Seite „Utilities” (Dienstprogramme) können Sie verschiedene Parameter des Routers einstellen und bestimmte administrative Aufgaben durchführen.



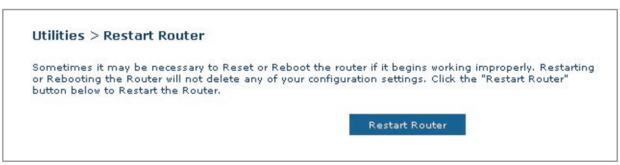
Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Reset Router**
  Sometimes it may be necessary to Reset or Reboot the router if it begins working improperly. Resetting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Default**
  Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Settings**
  You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Configuration**
  This option will allow you to restore a previously saved configuration.
- **Firmware Update**
  From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
- **System Settings**
  The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the NAT function of the Router.

Neustart Router

Bisweilen kann es notwendig sein, den Router zurückzusetzen oder neu zu starten, falls dieser nicht mehr erwartungsgemäß funktioniert. Bei einem Neustart bleiben die Konfigurationseinstellungen erhalten.



Utilities > Restart Router

Sometimes it may be necessary to Reset or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.

Restart Router

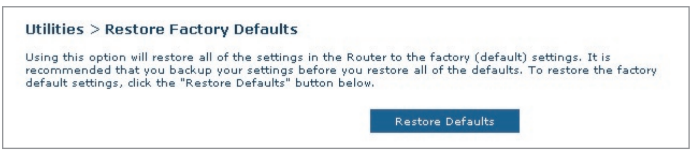
Wiederherstellen des Normalbetriebs durch einen Neustart

1. Klicken Sie auf die Schaltfläche „Restart Router” (Router neu starten).
2. Das folgende Meldungsfenster wird geöffnet. Klicken Sie auf „OK”, um den Router neu zu starten.

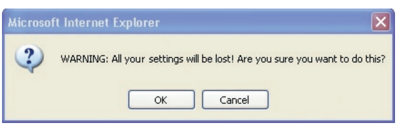


Werkseinstellungen wiederherstellen

Mit dieser Option setzen Sie alle Routereinstellungen auf die Werkseinstellungen zurück. Es wird empfohlen, die aktuellen Einstellungen zu sichern, bevor Sie die Werkseinstellungen wiederherstellen.

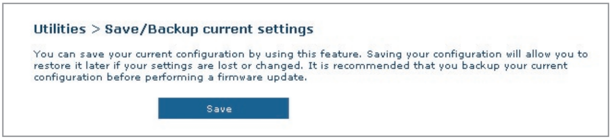


1. Klicken Sie auf die Schaltfläche „Restore Defaults” (Werkseinstellungen wiederherstellen).
2. Das folgende Meldungsfenster wird geöffnet. Klicken Sie auf „OK”, um die Werkseinstellungen wiederherzustellen.

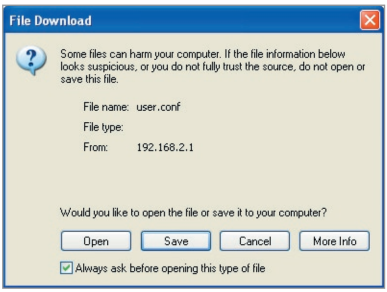


Aktuelle Einstellungen sichern / Sicherheitskopie erstellen

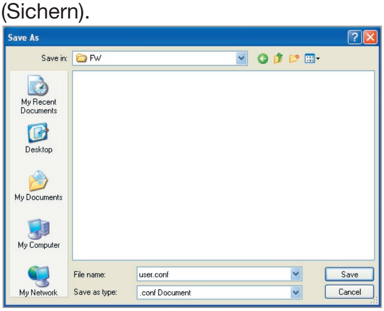
Mit dieser Funktion können Sie die aktuelle Konfiguration sichern. Dadurch können Sie Ihre Konfigurierung später wiederherstellen, wenn die Einstellungen zwischenzeitlich verloren gehen oder geändert werden. Sie sollten die aktuelle Konfiguration sichern, bevor Sie ein Firmware-Upgrade durchführen.



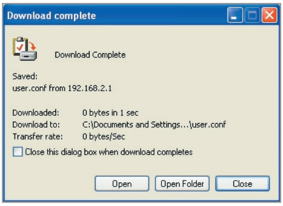
1. Klicken Sie auf „Save” (Sichern). Das Fenster „File Download” (Datei herunterladen) wird geöffnet. Klicken Sie auf „Save” (Sichern).



2. Es wird ein Fenster geöffnet, in dem Sie den Speicherort der Konfigurationsdatei festlegen können. Legen Sie den Pfad fest. Es gibt keine Beschränkungen bezüglich des Dateinamens, dennoch sollten Sie der Datei einen Namen geben, damit Sie sie später wiederfinden. Wenn Sie Pfad und Namen der Datei festgelegt haben, klicken Sie auf „Save” (Sichern).



3. Nach dem Sichern erscheint das folgende Fenster.
Klicken Sie auf „Close “ (Schließen).

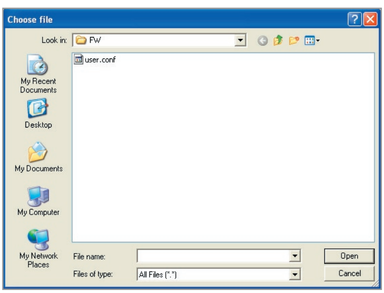


Die Konfiguration ist jetzt gesichert.

Vorherige Einstellungen wiederherstellen

Über diese Option stellen Sie die zuvor gespeicherten Einstellungen wieder her.

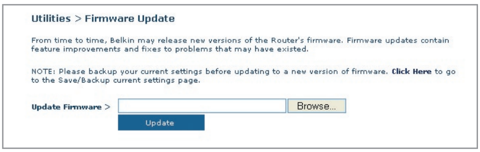
1. Klicken Sie auf „Browse” (Durchsuchen). Es wird ein Fenster geöffnet, in dem Sie den Pfad der Konfigurationsdatei festlegen können. Alle Konfigurationsdateien haben die Dateinamenerweiterung „.conf”. Klicken Sie die Konfigurationsdatei, die Sie wiederherstellen möchten, doppelt an.



2. Klicken Sie dann auf „Open” (Öffnen).

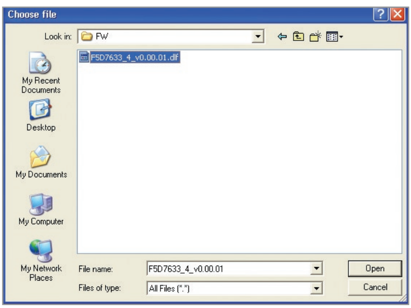
Firmware aktualisieren

Von Zeit zu Zeit veröffentlicht Belkin neue Versionen der Router-Firmware. Firmware-Aktualisierungen enthalten verbesserte Funktionen und Lösungen für eventuelle Probleme. Wenn Belkin eine neue Firmware veröffentlicht, können Sie diese von der Belkin Website herunterladen und die Firmware Ihres Routers auf den neuesten Stand bringen.



Aktualisieren der Router-Firmware

1. Klicken Sie auf der Seite „Firmware Update” (Aktualisieren der Firmware) auf „Browse” (Durchsuchen). Es wird ein Fenster geöffnet, in dem Sie den Pfad der Firmware-Aktualisierungsdatei wählen können.



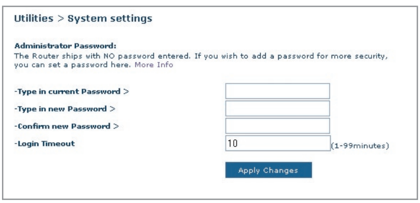
2. Suchen Sie die Firmware-Datei, die Sie heruntergeladen haben. Doppelklicken Sie auf den Dateinamen.
3. Klicken Sie auf „Update” (Aktualisieren), um die aktuellste Firmware-Version zu installieren.

Systemeinstellungen

Auf der Seite „System Settings” (Systemeinstellungen) können Sie ein neues Administratorkennwort festlegen, die Zeitzone einstellen, die Fernverwaltung aktivieren und die UPnP-Funktion des Routers ein- oder ausschalten.

Einstellen oder Ändern des Administratorkennworts

Der Router wird OHNE festgelegtes Kennwort geliefert. Sie können auf dieser Seite ein Kennwort festlegen und dadurch die Sicherheit erhöhen. Notieren Sie sich das Kennwort, und bewahren Sie es sicher auf. Sie benötigen es, wenn Sie sich künftig am Router anmelden möchten. Sie sollten ein Kennwort festlegen, wenn Sie die Fernverwaltung des Routers nutzen möchten.



Ändern der Einstellung für das Anmeldezeitlimit

Das Zeitlimit für die Anmeldung ermöglicht Ihnen, einen Zeitraum zu bestimmen, in der Sie für die Erweiterte Benutzeroberfläche des Routers angemeldet sind. Die Zähluhr startet, wenn keine Aktivität mehr registriert wird. Beispiel: Sie haben Änderungen mit der erweiterten Konfigurationsoberfläche vorgenommen und verlassen Ihren Arbeitsplatz, ohne auf „Logout” (Abmelden) zu klicken. Angenommen, das Zeitlimit ist auf 10 Minuten eingestellt; dann wird die angemeldete Sitzung nach 10 Minuten abgemeldet. Sie müssen sich dann erneut anmelden, um weitere Änderungen durchzuführen. Das Zeitlimit für die Anmeldung dient der Sicherheit und ist auf 10 Minuten voreingestellt.

Hinweis: Es kann jeweils nur ein Computer an der Erweiterten Benutzeroberfläche zur Routerkonfiguration angemeldet sein.

Einstellen von Uhrzeit und Zeitzone

Der Router hält die Uhrzeit auf dem Laufenden, indem er sich mit einem Simple Network Time Protocol (SNTP)-Server verbindet. Dadurch kann der Router die Systemuhr mit dem weltweiten Internet synchronisieren. Die synchronisierte Routeruhr dient zur Aufzeichnung des Sicherheitsprotokolls und zur Steuerung des Client-Filters.

Wählen Sie den gewünschten NTP-Zeitserver und die Zeitzone Ihres Wohnorts; klicken Sie dann auf „Apply Changes" (Änderungen übernehmen). Die Systemuhr wird nicht immer sofort aktualisiert. Sie müssen mindestens 15 Minuten abwarten, bis der Router die Zeitserver im Internet abfragt und eine Antwort erhält. Sie können die Uhr nicht selbst einstellen.



Aktivieren der Fernverwaltung

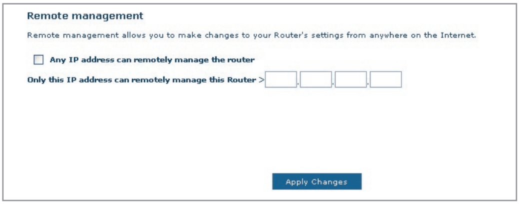
Bevor Sie diese Funktion des Belkin Routers aktivieren, **STELLEN SIE SICHER, DASS SIE DAS ADMINISTRATORENKENNWORT EINGESTELLT HABEN.**. Die Fernverwaltung ermöglicht das Ändern Ihrer Routereinstellungen von jedem Ort aus, an dem sich ein Internet-Anschluss befindet.

Klicken Sie auf die Schaltfläche „Change Settings" (Einstellungen Ändern), um die Seite „Remote Management" (Fernverwaltung) aufzurufen.

Für die Fernverwaltung des Routers gibt es zwei Methoden. Die erste Möglichkeit ist, den Zugriff auf den Router von überall aus dem Internet zuzulassen. Dazu wählen Sie die Option „Any IP address can remotely manage the Router" (Jede IP-Adresse ist zum Fernmanagement des Routers berechtigt). Wenn Sie Ihre WAN-IP-Adresse an einem beliebigen Computer im Internet eingeben, erscheint ein Anmeldefenster, in dem Sie Ihr Routerkennwort eingeben müssen.

Zum anderen können Sie eine bestimmte IP-Adresse festlegen, an der Sie die Fernverwaltung des Routers durchführen möchten. Dies ist sicherer, aber auch unpraktischer. Geben Sie für diese Methode die IP-Adresse des Computers, an dem Sie den Router fernverwalten möchten, in das entsprechende Feld ein, und aktivieren Sie die Option „Only this IP address can remotely manage the Router" (Nur mit dieser IP-Adresse kann der Router fernverwaltet werden). Bevor Sie diese Funktion aktivieren, sollten Sie UNBEDINGT ein Administratorenkennwort festlegen! Wenn Sie auf das Kennwort verzichten, setzen Sie Ihren Router der Gefahr von Manipulationen durch Unbefugte aus.

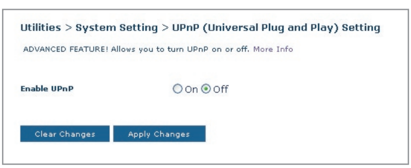
Klicken Sie auf „Apply Changes”, um die Änderungen zu sichern .



Aktivieren/Deaktivieren von UPnP

UPnP (Universelles Plug&Play) ist eine weitere erweiterte Funktion Ihres Belkin Routers. Diese Technologie ermöglicht den nahtlosen Betrieb von Sprach- und Videomeldungen, Spielen und anderen Anwendungen, die dem UPnP-Standard entsprechen. Für bestimmte Anwendungen muss die Router-Firewall auf eine ganz bestimmte Weise konfiguriert werden, damit sie störungsfrei funktionieren. Hierzu müssen meistens TCP- und UDP-Ports geöffnet und in bestimmten Fällen auch Trigger-Ports gesetzt werden. UPnP-kompatible Anwendungen können mit dem Router kommunizieren und ihm mitteilen, wie die Firewall konfiguriert werden muss. Werkseitig ist die UPnP-Funktion des Routers deaktiviert. Wenn Sie UPnP-kompatible Anwendungen einsetzen und die UPnP-Funktionen nutzen möchten, können Sie die UPnP-Option aktivieren.

Klicken Sie auf die Schaltfläche „Change Settings” (Einstellungen Ändern), um die Seite „Remote Management” (Fernverwaltung) aufzurufen. Wählen Sie dann „On” (An) bei „Enable UPnP” (UPNP aktivieren) zum Aktivieren von UPnP. Klicken Sie auf „Apply Changes”, um die Änderungen zu sichern .



Problem:

Die ADSL-Statusanzeige ist nicht an.

Lösung:

1. Überprüfen Sie die Verbindung zwischen Router- und ADSL-Leitung. Stellen Sie sicher, dass das ADSL-Kabel an den Port des Routers angeschlossen ist, der mit „DSL Line” (DSL-Leitung) bezeichnet ist.
2. Überprüfen Sie, ob der Router mit Strom versorgt wird. Die Betriebsanzeige ⏻ auf der Vorderseite sollte leuchten.

Problem:

Die Internet-Statusanzeige ist nicht an.

Lösung:

1. Stellen Sie sicher, dass das ADSL-Kabel an den Port des Routers angeschlossen ist, der mit „DSL Line” (DSL-Leitung) bezeichnet ist und dass die ADSL-Anzeige ☎ leuchtet.
2. Stellen Sie sicher, dass Sie die richtige VPI/VCI, den richtigen Benutzernamen und das korrekte Kennwort Ihres ISP (Internetproviders) verwenden.

Problem:

Ich arbeite mit einer statischen IP-Adresse. Ich kann keine Verbindung zum Internet herstellen.

Lösung:

Da Sie mit statischer IP-Adressierung arbeiten, muss Ihnen der Provider die IP-Adresse, die Subnet Mask und die Gateway-Adresse zuweisen. Verwenden Sie an Stelle des Assistenten den „Connection Type” (Verbindungstyp) und wählen Sie Ihre Verbindung aus. Klicken Sie auf „Next” (Weiter), wählen Sie „Static IP” (Statische IP-Adresse) und geben Sie Ihre IP-Adresse, Subnet-Mask und die Standard-Gateway-Daten ein.

Problem:

Ich habe mein Kennwort vergessen oder verloren.

Lösung:

Halten Sie den Schalter „Reset” (Zurücksetzen) auf der Rückseite für mindestens 10 Sekunden gedrückt, um die Werkseinstellung wieder herzustellen.

Problem:

Mein kabelloser PC kann keine Verbindung mit dem Router herstellen.

Lösung:

1. Stellen Sie sicher, dass Ihr kabelloser PC die gleichen SSID-Einstellungen wie der Router hat und ob auf den Clients die gleichen Sicherheitseinstellungen wie WPA- und WEP-Verschlüsselung vorhanden sind.
2. Stellen Sie sicher, das die Entfernung zwischen dem Router und dem kabellosen PC nicht zu groß ist.

Problem:

Das kabellose Netzwerk ist oft unterbrochen.

Lösung:

1. Stellen Sie Ihren kabellosen PC näher an den Router, um ein besseres Signal zu erhalten.
2. Es könnten auch Interferenzen vorhanden sein, die vermutlich durch eine Mikrowelle oder schnurlose Telefone mit 2.4GHz verursacht werden. Ändern Sie den Standort des Routers oder benutzen Sie einen anderen Funkkanal.

Problem:

Ich kann keine Funkverbindung zum Internet herstellen.

Lösung:

Wenn Sie mit einem kabellosen Computer keine Internetverbindung aufbauen können, prüfen Sie bitte Folgendes:

1. Schauen Sie auf die Lämpchen Ihres Routers. Wenn Sie einen Belkin Router verwenden, sollten die Lämpchen wie folgts ein:
   - Die Betriebsanzeige sollte leuchten.
   - Die DSL-Anzeige sollte an sein aber nicht blinken.
   - Die Internet-Anzeige sollte entweder an sein oder blinken.
2. Klicken Sie in der rechten unteren Ecke des Bildschirms im System-Tray auf das Symbol des Dienstprogramms für kabellose Netzwerke und öffnen Sie es. Wenn Sie eine kabellose Netzwerkkarte von Belkin benutzen, sollte das Symbol dieser Abbildung gleichen.  Das Symbol kann rot oder grün sein.
3. Welches Fenstergenau angezeigt wird, hängt von dem Modell Ihrer kabellosen Netzwerkkarte ab; jedesdieser Dienstprogramme verfügt über eine Liste verfügbarer Netzwerke (Available Networks) — kabellose Netzwerke, mit denen es eine Verbindung herstellen kann.

Wird der Name Ihres kabellosen Netzwerks in der Liste angezeigt?

Ja, in der Liste ist mein Netzwerkname aufgeführt—beachten Sie die Lösung im Abschnitt „Ich kann keine kabellose Internetverbindung aufbauen, aber mein Netzwerkname wird angezeigt" in diesem Kapitel (Fehlerbehebung).

Nein, in der Liste ist mein Netzwerkname nicht aufgeführt—beachten Sie den Abschnitt „Ich kann keine kabellose Internetverbindung aufbauen und mein Netzwerkname wird nicht angezeigt" in diesem Kapitel (Fehlerbehebung).

Problem:

Ich kann keine kabellose Internetverbindung aufbauen aber mein Netzwerkname wird angezeigt.

Lösung:

Ist Ihr Netzwerkname in der Liste der verfügbaren Netzwerke zu sehen, folgen Sie bitte diesen Schritten, um die Verbindung einzurichten:

1. Klicken Sie in der Liste „Verfügbare Netzwerke" auf den korrekten Netzwerknamen.
2. Ist die Sicherheitsfunktion (Verschlüsselung) aktiviert, müssen Sie den Netzwerkschlüssel eingeben. Weitere Informationen zur Sicherheit finden Sie auf der Seite mit dem Titel: „Änderungen der Sicherheitseinstellungen des Funknetzwerks".
3. Nach wenigen Sekunden sollte das Symbol in der linken unteren Bildschirmecke grün leuchten, ein Zeichen dafür, dass eine Verbindung zum Netzwerk aufgebaut wurde.



Problem:

Ich kann keine kabellose Internetverbindung aufbauen und mein Netzwerkname wird nicht angezeigt.

Lösung

Wenn der korrekte Netzwerkname nicht auf der Liste für „Available Networks" (Verfügbare Netzwerke) steht, folgen Sie bitte den folgenden Schritten zur Fehlersuche:

1. Stellen Sie den Computer, wenn möglich, zeitweilig im Abstand von etwa ein bis drei Metern vom Router auf. Schließen Sie das Dienstprogramm für kabellose Netzwerke und öffnen Sie es erneut. Wenn der korrekte

Netzwerkname jetzt auf der Liste für „Available Networks” (Verfügbare Netzwerke) erscheint, ist das Problem möglicherweise auf die Reichweite oder eine Störung zurückzuführen. Beachten Sie bitte die Lösungsvorschläge in Anhang B mit dem Titel „Wichtige Faktoren bei Aufstellung und Einrichtung”.

2. Wird ein Computer verwendet, der mit einem Netzwerkkabel an den Router angeschlossen ist (im Gegensatz zur kabellosen Verbindung), prüfen Sie ob „Broadcast SSID” (SSID rundsenden) aktiviert ist. Diese Einstellung ist auf der Seite für „Channel and SSID”- (Kanal und SSID) Einstellungen des Routers zu finden.

   Wenn Sie nach diesen Schritten weiterhin keine Internetverbindung aufbauen können, melden Sie sich bitte beim technischen Support von Belkin.

Problem:

Mein kabelloses Netzwerk arbeitet nicht konsistent.

Die Datenübertragung ist manchmal langsam.

Die Signalstärke ist unzureichend.

Es ist schwierig, eine Virtual Private Network (VPN)-Verbindung aufzubauen und/oder aufrechtzuerhalten.

Lösung:

Funktechnologie basiert auf Radiotechnik. Das bedeutet, dass die Verbindungsqualität und die Funktionalität zwischen den Geräten abnimmt, wenn die Entfernung zwischen den Geräten zunimmt. Andere Faktoren, die zur Verschlechterung des Signals führen können, sind Hindernisse wie Wände und Metallvorrichtungen (gerade Metall ist ein großer Störfaktor). Daraus ergibt sich in geschlossenen Räumen eine durchschnittliche Reichweite für kabellose Netzwerkgeräte von 30 bis 60 Metern. Bitte beachten Sie, dass die Verbindun gsgeschwindigkeit abnehmen kann, wenn Sie weiter vom Router oder Access Point entfernt sind.

Um zu prüfen, ob die Funkprobleme mit der Entfernung zu tun haben, stellen Sie den Computer zeitweilig, wenn möglich, in etwa ein bis drei Metern vom Router auf.

Wechseln des Funkkanals - Wenn Störungen auftreten, z.B. durch andere kabellose Netzwerke in der Umgebung, können Sie die Leistung und Verlässlichkeit Ihres Netzwerks verbessern, indem Sie den Kanal Ihres kabellosen Netzwerks wechseln. Der Standard-Kanal Ihres Routers ist werksbedingt auf 11 eingestellt, Sie können, je nach Region, aus diversen anderen Kanälen auswählen. Bitte beachten Sie hierzu auf Seite 35 den Abschnitt „Wechseln des Funkkanals”, um andere Kanäle einzustellen.

Verringerung der Übertragungsrate des kabellosen Netzwerks
- Verringerung der Übertragungsrate des kabellosen Netzwerks kann die maximale Reichweite des kabellosen Netzwerks und die Stabilität der Verbindung verbessern. Bei vielen kabellosen Netzwerkkarten kann die Übertragungsrate verringert werden. Gehen Sie hierfür zur Systemsteuerung von Windows, öffnen Sie die Netzwerkverbindungen und klicken Sie doppelt auf die Verbindung Ihrer kabellosen Netzwerkkarte. Wählen Sie im Dialogfeld „Eigenschaften” auf der Registerkarte „Allgemein” den Konfigurationsschalter aus (Anwender von Windows 98 müssen die kabellose Netzwerkkarte im Listenfeld auswählen und dann auf „Eigenschaften” klicken), wählen Sie den Schalter „Erweitert” und anschließend die entsprechende Übertragungsrate. Kabellose Client-Karten sind normalerweise so eingestellt, dass sie die Übertragungsrate automatisch anpassen; dies kann allerdings zu periodischen Unterbrechungen führen, wenn das Funksignal zu schwach ist; langsamere Übertragungsraten sind in der Regel stabiler. Probieren Sie verschiedene Übertragungsraten aus, bis Sie die passende für Ihre Umgebung gefunden haben; bitte beachten Sie, dass die Übertragungsraten für den Internetgebrauch anwendbar sein müssen. Beachten Sie für weitere Informationen das Handbuch Ihrer kabellosen Netzwerkkarte.

Problem:

Ich habe Schwierigkeiten beim Einstellen der Wired Equivalent Privacy (WEP) auf einem Router oder Access Point von Belkin.

Lösung

1. Melden Sie sich bei Ihrem kabellosen Router oder Access Point an.
2. Öffnen Sie Ihren Internet-Browser und tragen Sie die IP-Adresse des kabellosen Routers oder Access Points ein.. (Beim Router ist dies standardmäßig 192.168.2.1, beim 802.11g Access Point ist dies 192.168.2.254). Melden Sie sich bei Ihrem Router durch Klicken auf den Schalter „Login” (Anmelden) in der oberen rechten Ecke des Bildschirms an. Sie werden nach Ihrem Kennwort gefragt. Wenn Sie noch kein Kennwort eingestellt haben, lassen Sie das Feld frei und klicken Sie auf „Submit” (Abschicken).
3. Klicken Sie links im Bildschirm auf den Schalter „Wireless” (Funknetz). Wählen Sie „Encryption” (Verschlüsselung) oder „Security” (Sicherheit), um zur Sicherh eitseinstellungsseite zu gelangen.
4. Wählen Sie im Dropdown-Menü die Option „128-bit WEP”.
5. Nachdem Sie den WEP-Verschlüsselungsmodus gewählt haben, können Sie den HEX WEP-Schlüssel manuell eingeben oder ein Kennwort in das Feld „Passphrase” (Kennfolge) eingeben und auf „Generate” (Generieren)

klicken, um aus der Kennfolge automatisch einen WEP-Schlüssel zu erstellen. Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten. Ein Hexadezimalschlüssel ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0-9. Für 128-Bit-WEP müssen Sie 26 Hexadezimalzeichen eingeben.

Beispiel:
C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-Bit-Schlüssel

6. Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um abzuschließen. Die Verschlüsselung ist nun im kabellosen Router eingestellt. Jeder Computer in Ihrem kabellosen Netzwerk muss jetzt mit denselben Sicherheitseinstellungen konfiguriert werden.

ACHTUNG: Wenn Sie für die Einstellung einen Computer benutzen, der mit einem kabellosen Router oder Access Point verbunden ist, vergewissern Sie sich, dass die Sicherheitsfunktion für diesen Client aktiviert ist. Falls dies nicht der Fall ist, wird die Funkverbindung unterbrochen.

Hinweis an Mac-Benutzer: Apple AirPort®-Produkte unterstützen in der Original-Ausführung nur Verschlüsselung mit 64 Bit. Apple AirPort 2-Produkte unterstützen sowohl 64-Bit- als auch 128-Bit-Verschlüsselung. Bitte überprüfen Sie Ihr Apple Airport-Produkt, um die verwendete Version festzustellen. Wenn Sie Ihr Netzwerk nicht mit 128 Bit verschlüsseln können, sollten Sie es mit der 64-Bit-Verschlüsselung probieren.

Problem:

Ich habe Schwierigkeiten beim Einstellen der Wired Equivalent Privacy (WEP) auf einer kabellosen Netzwerkkarte von Belkin.

Lösung:

Die kabellose Netzwerkkarte muss den gleichen Schlüssel wie der kabellose Router oder Access Point verwenden. Benutzt Ihr kabelloser Router oder Access Point z. B. den Schlüssel 00112233445566778899AABBCC, muss die kabellose Netzwerkkarte exakt auf den gleichen Schlüssel eingestellt werden.

1. Klicken Sie doppelt auf die Signalanzeige, um das Dienstprogramm für kabellose Netzwerke zu starten.
2. Mit der Schaltfläche „Advanced” (Weitere Optionen) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
3. Sobald die Schaltfläche „Advanced” (Weitere Optionen) geklickt ist, erscheint das LAN-Dienstprogramm von Belkin. Das Dienstprogramm erlaubt Ihnen die Verwaltung aller erweiterter Funktionen der kabellosen Netzwerkkarte von Belkin.
4. Wählen Sie auf der Registerkarte „Wireless Network Properties”

(Netzwerkeigenschaften) einen Netzwerknamen aus der Liste „Available networks” (verfügbare Netzwerke) aus und klicken Sie auf „Properties” (Eigenschaften).

5. Wählen Sie bei „Data Encryption” (Datenverschlüsselung) „WEP”.
6. Das untere Feld „Network key is provided for me automatically” (Netzwerkschlüssel wird automatisch vergeben) darf nicht aktiviert sein. Wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk herzustellen, wenden Sie sich bitte an Ihren Netzwerkadministrator für den Fall, dass dieses Feld aktiviert werden muss.
7. Geben Sie Ihren WEP-Schlüssel in das Feld „Network Key” (Netzwerkschlüssel) ein.

   Wichtiger Hinweis: Ein WEP-Schlüssel ist eine Kombination aus Zahlen und Buchstaben von A-F und 0-9. Für 128-Bit WEP müssen Sie 26 Schlüssel eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres kabellosen Routers oder Access Points übereinstimmen..

   Beispiel:

   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-Bit-Schlüssel
8. Klicken Sie auf „OK”, und dann auf „Apply” (Übernehmen), um die Einstellungen zu sichern.

Wenn Sie **KEINE** kabellose Netzwerkkarte von Belkin benutzen, melden Sie sich bitte beim Hersteller Ihrer Netzwerkkarte, um das Benutzerhandbuch für die Karte zu erhalten.

Problem:

Unterstützen die Produkte von Belkin WPA?

Lösung

Hinweis: Um WPA zu verwenden, müssen alle Ihre Clients auf die Software und Treiber, die WPA unterstützen, aktualisiert sein. Zum Zeitpunkt der Erstellung dieser Anleitung ist von Microsoft ein kostenloses Sicherheitspatch als Download erhältlich. Dieses Patch gilt nur für das Betriebssystem Windows XP.

Laden Sie sich das Patch hier herunter:

http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

Sie benötigen auch die aktuellen Treiber von Belkin für Ihre kabellose 802.11g Desktop- oder Notebook-Netzwerkkarte. Diese finden Sie auf der Support-Internetseite von Belkin. Andere Betriebssysteme können zur Zeit nicht unterstützt werden. Das Patch von Microsoft unterstützt nur Geräte mit WPA-aktivierten Treibern, wie die 802.11g-Produkte von Belkin.

Laden Sie die aktuellen Treiber hier herunter: http://web.belkin.com/support/networkingsupport.asp.

WPA-Unterstützung wird automatisch durch den Upgrade Ihres Systems auf Windows XP Service Pack 2 installiert. Weitere Informationen hierzu finden Sie unter: http://support.microsoft.com

Problem:

Ich habe in einem Heimnetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einem Router oder Access Point von Belkin.

Lösung:

1. Wählen Sie im Dropdown-Menü „Security Mode" (Sicherheitsmodus) „WPA-PSK (no server)" (WPA-PSK (kein Server)) aus.
2. Wählen Sie als Verschlüsselungstechnik „TKIP" oder „AES" aus. Diese Einstellungen müssen mit denen Ihrer Clients übereinstimmen.
3. Geben Sie Ihren Pre-Shared Key (PSK) ein . Dieser kann aus acht bis 63 Zeichen (Buchstaben, Zahlen, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten. Ihr PSK kann zum Beispiel heißen: „Familie Manns Netzwerkschlüssel".
4. Klicken Sie auf „Apply Changes" (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.

Problem:

Ich habe in einem Firmennetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einem Router oder Access Point von Belkin.

Lösung:

Wenn Sie in Ihrem Netzwerk einen Radius-Server verwenden, um die Schlüssel an die Clients zu verteilen, verwenden Sie diese Einstellung. Diese Technik wird typischerweise in einer Unternehmensumgebung eingesetzt.

1. Wählen Sie im Dropdown-Menü „Security Mode" (Sicherheitsmodus) „WPA (with server)" (WPA [mit Server]) aus.
2. Wählen Sie als Verschlüsselungstechnik „TKIP" oder „AES" aus. Diese Einstellungen müssen mit denen Ihrer Clients übereinstimmen.
3. Geben Sie die IP-Adresse des Radius-Servers in die Felder unter „Radius Server" ein.
4. Geben Sie den Radius-Schlüssel in das Feld „Radius Key" (Radius-Schlüssel) ein.
5. Geben Sie das Schlüsselintervall ein. Das Schlüsselintervall gibt an, wie oft die Schlüssel verteilt werden (in Paketen).
6. Klicken Sie auf „Apply Changes" (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.

Problem:

Ich habe in einem Heimnetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einer kabellosen Netzwerkkarte von Belkin..

Lösung:

Die Clients müssen den gleichen Schlüssel wie der kabellose Router oder Access Point verwenden. Heißt der Schlüssel im kabellosen Router oder Access Point z.B. „Familie Manns Netzwerkschlüssel”, müssen die Clients den gleichen Schlüssel verwenden.

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network” (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen.
2. Mit der Schaltfläche „Advanced” (Weitere Optionen) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
3. Sobald die Schaltfläche „Advanced” (Weitere Optionen) geklickt ist, erscheint das LAN-Programm für kabellose Netzwerke von Belkin. Das Dienstprogramm erlaubt Ihnen die Verwaltung aller erweiterter Funktionen der kabellosen Netzwerkkarte von Belkin.
4. Wählen Sie auf der Registerkarte „Wireless Network Properties” (Netzwerkeigenschaften) einen Netzwerknamen aus der Liste „Available networks” (verfügbare Netzwerke) aus und klicken Sie auf „Properties” (Eigenschaften).
5. Wählen Sie unter „Network Authentication” (Netzwerk-Authentifizierung) den Eintrag „WPA-PSK (No Server)” (WPA-PSK [KeinServer]) aus.
6. Geben Sie Ihren WPA-Schlüssel in das Feld „Network Key” (Netzwerkschlüssel) ein.

Wichtig: Ein WPA-PSK ist eine Kombination aus Zahlen und Buchstaben von A-Z und 0-9. Für WPA-PSK können Sie acht bis 63 Zeichen eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres kabellosen Routers übereinstimmen.

7. Klicken Sie auf „OK”, und dann auf „Apply” (Übernehmen), um die Einstellungen zu sichern.

Problem:

Ich habe in einem Firmennetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einer kabellosen Netzwerkkarte von Belkin.

Lösung:

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network” (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen.
2. Mit der Schaltfläche „Advanced” (Weitere Optionen) können Sie zusätzliche Kartenoptionen überprüfen und verändern.

3. Sobald die Schaltfläche „Advanced" (Weitere Optionen) geklickt ist, erscheint das LAN-Programm für kabellose Netzwerke von Belkin. Das Dienstprogramm erlaubt Ihnen die Verwaltung aller erweiterter Funktionen der kabellosen Netzwerkkarte von Belkin.
4. Wählen Sie auf der Registerkarte „Wireless Network Properties" (Netzwerkeigenschaften) einen Netzwerknamen aus der Liste „Available networks" (Verfügbare Netzwerke) aus und klicken Sie auf „Properties" (Eigenschaften).
5. Wählen Sie unter „Network Authentication" (Netzwerk-Authentifizierung) den Eintrag „WPA" aus.
6. Wählen Sie auf der Registerkarte „Authentication" (Authentifizierung) die Einstellungen, die Ihnen von Ihrem Netzwerkadministrator angegeben werden.
7. Klicken Sie auf „OK", und dann auf „Apply" (Übernehmen), um die Einstellungen zu speichern.

Problem:

Ich habe in einem Heimnetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) und ich benutze **KEINE** kabellose Netzwerkkarte von Belkin.

Lösung:

Wenn Sie **KEINE** kabellose Netzwerkkarte von Belkin benutzen und Ihre kabellose Desktop- und Notebookkarte nicht mit WPA-Software ausgestattet ist, kann ein Sicherheitspatch von Microsoft mit dem Namen „Windows XP Support Patch for Wireless Protected Access" kostenlos heruntergeladen werden. Suchen Sie in der Unterstützungsdatenbank von Microsoft unter dem Suchwort Windows XP WPA und laden Sie das Patch herunter.

Hinweis: Dieses von Microsoft zur Verfügung gestellte Patch gilt nur für das Betriebssystem Windows XP. Andere Betriebssysteme können zur Zeit nicht unterstützt werden. Sie müssen auch überprüfen, ob der Hersteller der kabellosen Karte WPA unterstützt und Sie die aktuellsten Treiber heruntergeladen und installiert haben.

Unterstützte Betriebssysteme:

- Windows XP Professional
- Windows XP Home Edition

WPA-PSK (kein Server) aktivieren

1. Unter Windows XP, klicken Sie auf „Start > Systemsteuerung > Netzwerkverbindungen".
2. Klicken Sie mit der rechten Maustaste auf „Drahtlose Netzwerke" (Wireless Networks). Das folgende Fenster wird angezeigt. Vergewissern Sie sich, dass das Feld „Use Windows to configure my wireless network settings" (Windows zum Konfigurieren der Einstellungen verwenden) aktiviert ist.
3. Klicken Sie auf der Registerkarte „Wireless Networks" (Drahtlose Netzwerke) auf die Schaltfläche „Configure" (Konfigurieren). Das folgende Fenster wird

angezeigt.

4. Nutzer von Heim- oder kleinen Unternehmensnetzwerken wählen „WPA-PSK" unter „Network Administration" (Netzwerkverwaltung).

Hinweis: Wählen Sie „WPA (with radius server)" (WPA [mit Radius-Server]) aus, wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk, das einen Authentifizierungsserver wie einen Radius-Server unterstützt, herzustellen. Wenden Sie sich für weitere Informationen bitte an Ihren Netzwerkadministrator.

5. Wählen Sie unter „Data Encryption" (Datenverschlüsselung) „TKIP" oder „AES". Diese Einstellungen müssen identisch mit denen Ihres kabellosen Routers oder Access Points sein.

6. Geben Sie Ihren Verschlüsselungsschlüssel in das Feld „Network Key" (Netzwerkschlüssel) ein.

Wichtig: Geben Sie Ihren Pre-Shared Key (PSK) ein. Er kann aus acht bis 63 Zeichen (Buchstaben, Ziffern, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten.

7. Klicken Sie auf „OK", um die Einstellungen zu übernehmen.

Was ist der Unterschied zwischen 802.11b, 802.11g, G+ MIMO und Pre-N?

Es gibt heutzutage vier verschiedene WLAN-Standards, die Daten bei sehr unterschiedlichen Höchstgeschwindigkeiten übertragen. Jede basiert auf der Zuweisung 802.11(x), benannt vom IEEE, dem Gremium, das für zertifizierte Netzwerkstandards verantwortlich ist. Der gebräuchlichste WLAN-Standard, 802.11b, überträgt Daten mit 11 Mbit/s; 802.11a und 802.11g arbeiten mit 54 Mbit/s, G+ MIMO arbeitet mit 54 Mbit/s und Pre-N mit 108 Mbit/s.

Vergleich zwischen verschiedenen WLAN-Standards

Funktechnologie	802.11b	G (802.11g)	G+ (802.11g mit HSM)	G+ MIMO(802.11g mit MIMO MRC)	Belkin Pre-N (802.11g mit TrueMIMO)
Geschwindigkeit*	11 Mbit/s Übertragungsrate / Basis	5 x schneller als der Standard 802.11b*	10 x schneller als der Standard 802.11b*	10 x schneller als der Standard 802.11b*	15 x schneller als der Standard 802.11b*
Frequenz	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen
Kompatibilität	Kompatibel zu 802.11g	Kompatibel mit 802.11b/g	Kompatibel mit 802.11b/g	Kompatibel mit 802.11b/g	Kompatibel mit 802.11g oder 802.11b
Reichweite*	normal 30-60 m in Innenräumen	Bis zu 120 m*	Bis zu 210 m*	Bis zu 300 m*	Bis zu 420 m*
Vorzug	Technisch ausgereift—bekannte Technologie	Bekannt—verbreitet bei der gemeinsamen Internetnutzung	Höhere Geschwindigkeit und bessere Funkabdeckung	Bessere Funkabdeckung und gleichmäßige Übertragungs geschwindigkeit	Brandneu—beste Funkabdeckung und Durchsatzleistung

*Reichweite und Verbindungsgeschwindigkeit sind abhängig von Ihrer Netzwerkumgebung.

Anhang A: Glossar

IP-Adresse

Diese „IP-Adresse" ist die interne IP-Adresse des Routers. Um die erweiterte Konfigurationsoberfläche zu öffnen, geben Sie diese IP-Adresse in die Adresszeile Ihres Browsers ein. Bei Bedarf können Sie die Adresse ändern. Geben Sie hierzu die neue IP-Adresse ein und klicken Sie auf „Apply Changes" (Änderungen übernehmen). Achten Sie darauf, dass Sie eine nicht routbare IP-Adresse wählen. Beispiele für nicht routbare IP-Adressen:

192.168.x.x (x steht für eine Zahl zwischen 0 und 255)

10.x.x.x (x steht für eine Zahl zwischen 0 und 255)

Subnet-Mask

Etliche Netzwerke sind zu groß, um den Datenverkehr in alle ihre Bereiche zuzulassen. Diese Netzwerke müssen in kleinere, überschaubarere Abschnitte aufgeteilt werden, sogenannte „Subnets" (Subnetze). Die Subnet-Mask ist die Netzwerkadresse plus der Information, die für die Identifizierung des „subnetwork" (Unternetzwerk) reserviert ist.

DNS

DNS ist die Abkürzung für Domain Name Server (Domänennamen-Server). Als DNS (Domain Name Server) wird ein Server im Internet bezeichnet, der URLs (Universal Resource Links) wie „www.belkin.com” zu IP-Adressen umwandelt. Bei vielen Providern ist eine Eingabe dieser Informationen in den Router unnötig. Wenn Sie einen statischen Verbindungstyp verwenden, müssen Sie möglicherweise eine bestimmte DNS-Adresse sowie eine sekundäre DNS-Adresse angeben, damit die Verbindung ordnungsgemäß funktioniert. Wenn Sie mit einem dynamischen Verbindungstyp oder PPPoE arbeiten, müssen Sie wahrscheinlich keine DNS-Adresse eingeben.

PPPoE

Die meisten DSL-Anbieter nutzen den Verbindungstyp PPPoE. Wenn Sie per ADSL-Modem mit dem Internet verbunden sind, erfolgt die Anmeldung an den Service des Providers möglicherweise über PPPoE.

Ihr Verbindungstyp ist PPPoE, wenn folgende Voraussetzungen zutreffen:

1. Ihr Internet-Provider hat Ihnen einen Benutzernamen und ein Kennwort für die Verbindung zum Internet zugewiesen.
2. Ihr Internetprovider hat Ihnen für die Internetverbindung Software wie WinPOET oder Enternet300 geliefert.
3. Sie müssen auf ein Desktop-Symbol doppelklicken (zusätzlich zum Browser), um ins Internet zu gelangen.

   Um den Router auf PPPoE einzurichten, geben Sie in den entsprechenden Feldern Ihren Benutzernamen und Ihr Kennwort ein. Klicken Sie nach der Eingabe Ihrer Informationen auf „Apply Changes” (Änderungen übernehmen).

Wenn Sie die Einstellungen übernommen haben, meldet die Statusanzeige „connection OK” (Verbindung OK), wenn der Router korrekt konfiguriert wurde.

PPPoA

Geben Sie die PPPoA Informationen in die vorgegebenen Felder und klicken Sie auf „Next” (Weiter). Klicken Sie auf „Apply” (Übernehmen), um Ihre Einstellungen zu aktivieren.

1. Benutzername - Geben Sie den Benutzernamen ein. (Vom Internetprovider vergeben).
2. Kennwort - Geben Sie Ihr Kennwort ein. (Vom Internetprovider vergeben).
3. Kennwort erneut eingeben - Bestätigen Sie das Kennwort. (Wird von Ihrem Internetprovider festgelegt).

4. VPI/VCI - Geben Sie Ihren Virtual Path Identifier (Virtuelle Pfaderkennung - VPI) und Virtual Circuit Identifier (Virtuelle Circuiterkennung - VCI) hier ein. (Vom Internetprovider vergeben).

Trennen nach X...

Die Funktion „Disconnect" dient zur automatischen Trennung des Routers vom Internet, wenn eine bestimmte Zeit lang keine Aktivität mehr festgestellt wird. Wenn Sie diese Option aktivieren und zum Beispiel „5" in das Feld „Minute" eingeben, wird der Router nach fünf Minuten Inaktivität vom Internet getrennt. Diese Option sollte nur verwendet werden, wenn Ihre Internet-Nutzung nach Zeit abgerechnet wird.

Kanal und SSID

Sie können den Betriebskanal des Routers wechseln. Wählen Sie hierzu den gewünschten neuen Kanal aus dem Dropdown-Menü. Klicken Sie auf „Apply Changes" (Änderungen übernehmen), um die Einstellung zu sichern. Sie können auch die SSID ändern. Die SSID entspricht dem Namen des kabellosen Netzwerks. Sie können die SSID frei festlegen. Wenn sich in der näheren Umgebung weitere kabellose Netzwerke befinden, müssen Sie dem Netzwerk einen eindeutigen Namen zuweisen. Klicken Sie in das SSID-Feld und geben Sie einen neuen Namen ein. Klicken Sie auf „Apply Changes" (Änderungen übernehmen), um die Änderung zu speichern.

ESSID Broadcast

Viele kabellose Netzwerkadapter, die zur Zeit auf dem Markt sind, verfügen über eine Funktion namens Standortübersicht. Sie überprüft die Umgebung nach verfügbaren Netzwerken und ermöglicht jedem Computer, automatisch ein Netzwerk in der Umgebung auszuwählen. Dies geschieht, wenn die SSID des Computers auf „ANY" (ALLE) steht. Ihr Belkin Router kann diese Zufallssuche nach einem Netzwerk blockieren. Wenn Sie die Funktion „ESSID Broadcast" deaktivieren, kann Ihr Computer nur dann in das Netzwerk, wenn seine SSID auf den Namen des Netzwerkes (wie WLAN) eingestellt wurde. Bevor Sie diese Option nutzen, sollten Sie sich vergewissern, dass Sie Ihre SSID (den Netzwerknamen) kennen. Sie können Ihr kabelloses Netzwerk fast unsichtbar machen. Wenn Sie das Rundsenden der SSID deaktivieren, wird Ihr Netzwerk nicht in Standortübersichten aufgenommen. Wenn Sie die Rundsendung der SSID deaktivieren, verbessern Sie die Netzwerksicherheit.

Verschlüsselung

Mit einer Verschlüsselung können Sie die Sicherheit Ihres Netzwerks verbessern. Der Router benutzt zwei Arten von Verschlüsselung: Wired Equivalent Privacy (WEP) und WIFI Protected Access (WPA), um Ihre Daten und Funktionen zu schützen. Die Verschlüsselung erfolgt mit 64- oder 128-Bit. Verschlüsselung

basiert auf mehreren Codeschlüsseln. Der Schlüssel des Computers muss mit dem des Routers übereinstimmen. Es gibt zwei Arten, einen Schlüssel zu erstellen. Die einfachste ist, die Software des Routers zum Umwandeln eines von Ihnen gewählten Kennwortes in einen Schlüssel zu benutzen. Alternativ hierzu können die Schlüssel auch manuell festgelegt werden.

Virtuelle Server

Mit dieser Funktion können Sie externe Aufrufe (aus dem Internet) von Diensten wie Webserver (Port 80), FTP-Server (Port 21) und andere Anwendungen über Ihren Router in das interne Netzwerk umleiten. Da Ihre internen Computer durch eine Firewall geschützt sind, kann auf diese aus dem Internet nicht zugegriffen werden, weil sie dort nicht „sichtbar" sind. Wenn Sie die virtuelle Serverfunktion für eine bestimmte Anwendung einstellen müssen, sollten Sie Kontakt zum Hersteller des Programms aufnehmen, um dort zu erfahren, welche Port-Einstellungen Sie vornehmen müssen.

Für die manuelle Eingabe, geben Sie die IP-Adresse in das vorgegebene Feld für interne Geräte, den Port Typ (TCP oder UDP) sowie die LAN und öffentlichen Ports, die passiert werden müssen, ein. Wählen Sie dann „Enable" (Aktivieren) und „Set" (Einstellen). Sie können pro interner IP-Adresse nur einen Port freigeben. Das Öffnen von Ports in Ihrer Firewall kann ein Sicherheitsrisiko darstellen. Das Aktivieren und Deaktivieren von Einstellungen geht schnell von der Hand. Daher sollten Sie die Einstellungen deaktivieren, wenn Sie eine bestimmte Anwendung momentan nicht verwenden.

Client-IP-Filter

Sie können den Router so einstellen, dass der Zugriff auf das Internet, E-Mail oder andere Netzwerke auf bestimmte Tage und Zeiten beschränkt wird. Die Beschränkung kann für einen einzelnen oder mehrere Computer festgelegt werden.

MAC Adress-Filter

Der MAC-Adressfilter ist eine leistungsstarke Sicherheitsfunktion, mit der Sie festlegen können, welche Computer für das Netzwerk zugelassen sind. Computern, die nicht in der Filterliste verzeichnet sind, wird der Zugriff auf das Netzwerk verweigert. Wenn Sie diese Funktion aktivieren, müssen Sie die MAC-Adresse eines jeden Clients auf Ihrem Netzwerk angeben, um den Netzwerkzugriff für diesen zu ermöglichen oder die MAC-Adresse kopieren, in dem Sie den Namen des Computers aus der „DHCP Client-Liste" auswählen. Um diese Funktion zu aktivieren, wählen Sie „Enable" (Aktivieren). Klicken Sie dann auf „Apply Changes" (Änderungen übernehmen), um die Einstellungen zu speichern.

DMZ

Wenn Sie einen Client-PC haben, auf dem hinter der Firewall keine Internetanwendung richtig ausgeführt werden kann, können Sie den Client für ungehinderten Internetzugriff einstellen. Das kann erforderlich sein, wenn die NAT-Funktion bei einer Anwendung Probleme verursacht, zum Beispiel bei einem Spiel oder einer Videokonferenzanwendung. Verwenden Sie diese Funktion nur zeitweise. **Der DMZ-Computer ist NICHT vor Hacker-Angriffen geschützt.**Um einen Computer in die DMZ zu versetzen, geben Sie die letzten Ziffern der LAN-IP-Adresse in das Feld für die statische IP-Adresse ein und klicken Sie auf „Apply Changes" (Änderungen übernehmen), um die Änderungen zu aktivieren.

Haben Sie nur eine öffentliche (WAN) IP-Adresse, können Sie diese öffentliche IP auf „0.0.0.0" stehen lassen. Wenn Sie mehrere öffentliche (WAN)-IP-Adressen verwenden, können Sie wählen, welche öffentliche (WAN)-IP-Adresse dem DMZ-Host zugewiesen werden soll. Geben Sie die öffentliche (WAN)-IP-Adresse ein, zu der der DMZ-Host umgeleitet werden soll, geben Sie die beiden letzten Ziffern der IP-Adresse des DMZ-Host-Computers ein und klicken Sie auf „Apply Changes" (Änderungen übernehmen).

Administratorkennwort

Der Router wird OHNE festgelegtes Kennwort geliefert. Wenn Sie zur Sicherheit ein Kennwort angeben möchten, können Sie dieses auf der webgestützten Benutzeroberfläche des Routers einstellen. Bewahren Sie das Kennwort sicher auf. Sie benötigen es, wenn Sie sich künftig am Router anmelden möchten. Es wird **DRINGEND EMPFOHLEN** ein Kennwort anzugeben, wenn Sie die Fernverwaltung des Routers benutzen wollen. Das Zeitlimit für die Anmeldung ermöglicht Ihnen, einen Zeitraum zu bestimmen, in der Sie für die Erweiterte Benutzeroberfläche des Routers angemeldet sind. Die Zähluhr startet, wenn keine Aktivität mehr registriert wird. Beispiel: Sie haben Änderungen mit der erweiterten Konfigurationsoberfläche vorgenommen und verlassen Ihren Arbeitsplatz, ohne auf „Logout" (Abmelden) zu klicken.

Angenommen, das Zeitlimit ist auf 10 Minuten eingestellt. Dann läuft die Anmeldesitzung 10 Minuten nach dem Verlassen ab. Sie müssen sich dann erneut anmelden, um weitere Änderungen durchzuführen. Das Zeitlimit für die Anmeldung dient der Sicherheit und ist auf 10 Minuten voreingestellt. Es kann jeweils nur ein Computer an der erweiterten Konfigurationsoberfläche zur Routerkonfiguration angemeldet sein.

Uhrzeit und Zeitzone

Der Router hält die Uhrzeit auf dem Laufenden, indem er sich mit einem Simple Network Time Protocol (SNTP)-Server verbindet. Dadurch kann der Router die Systemuhr mit dem weltweiten Internet synchronisieren. Die synchronisierte Routeruhr dient zur Aufzeichnung des Sicherheitsprotokolls und zur Steuerung des Client-Filters. Wählen Sie die Zeitzone, in der Sie sich befinden. Wenn Sie sich in einer Region befinden, in der zwischen Sommer- und Winterzeit umgestellt wird, markieren Sie das Feld neben „Enable Daylight Saving" (Sommerzeit aktivieren). Die Systemuhr wird nicht immer sofort aktualisiert. Sie müssen mindestens 15 Minuten abwarten, bis der Router die Zeitserver im Internet abfragt und eine Antwort erhält.

Fernverwaltung

Bevor Sie diese Funktion aktivieren, **SOLLTEN SIE UNBEDINGT EIN ADMINISTRATORKENNWORT FESTLEGEN**. Die Fernverwaltung ermöglicht das Ändern Ihrer Routereinstellungen von jedem Ort aus, an dem sich ein Internet-Anschluss befindet.

UPnP

Die UPnP-Technologie (Universales Plug&Play) ermöglicht den nahtlosen Betrieb von Sprach- und Videomeldungen, Spielen und anderen Anwendungen, die dem UPnP-Standard entsprechen. Für bestimmte Anwendungen muss die Router-Firewall auf eine ganz bestimmte Weise konfiguriert werden, damit sie störungsfrei funktionieren. Hierzu müssen meistens TCP- und UDP-Ports geöffnet und in bestimmten Fällen auch Trigger-Ports gesetzt werden. UPnP-kompatible Anwendungen können mit dem Router kommunizieren und ihm mitteilen, wie die Firewall konfiguriert werden muss.

Werkseitig ist die UPnP-Funktion des Routers deaktiviert. Wenn Sie UPnP-kompatible Anwendungen einsetzen und die UPnP-Funktionen nutzen möchten, können Sie die UPnP-Option aktivieren. Wählen Sie hierzu auf der Seite „Utilities” (Dienstprogramme) im Abschnitt „UPnP Enabling” (UPnP-Aktivierung) die Option „Enable” (Aktivieren). Klicken Sie auf „Apply Changes” (Änderungen übernehmen), um die Änderung zu speichern.

Anhang B: Wichtige Faktoren bei Aufstellung und Einrichtung

Hinweis: Obwohl manche der folgenden Faktoren die Funktion Ihres Netzwerks beeinträchtigen können, werden Sie Ihr kabelloses Netzwerk nicht völlig funktionsunfähig machen. Wenn Sie vermuten, dass Ihr Netzwerk nicht optimal funktioniert, kann Ihnen diese Kontrollliste helfen.

1. **Standort des kabellosen Routers oder Access Points**

   Stellen Sie Ihren kabellosen Router, den zentralen Verbindungspunkt Ihres Netzwerks, soweit wie möglich in den Mittelpunkt Ihrer kabellosen Netzwerkgeräte.

Um den besten Empfang für Ihre „kabellosen Clients" (d. h. Computer, die mit kabellosen Notebook- oder Desktop-Netzwerkkarten von Belkin oder kabellosen USB-Adaptern ausgestattet sind) zu bekommen:

- Stellen Sie sicher, dass die Antennen des kabellosen Routers oder Access Points parallel zueinander und vertikal aufgestellt sind (mit Ausrichtung auf die Decke). Wenn Ihr kabelloser Router (oder Access Point) vertikal aufgestellt ist, richten Sie die Antennen soweit wie möglich nach oben aus.
- Wenn sich Ihr Wohnraum über mehrere Etagen erstreckt, stellen Sie den kabellosen Router (oder Access Point) in einem Stockwerk auf, das im Gesamtwohnraum so zentral wie möglich gelegen ist. Dies kann bedeuten, dass Sie den kabellosen Router (oder Access Point) in einem der oberen Stockwerke aufstellen müssen.
- Stellen Sie den kabellosen Router (oder Access Point) nicht in der Nähe eines schnurlosen Telefons, das das 2,4-GHz-Band nutzt, auf.

2. **Vermeiden Sie Hindernisse und Störungsquellen**

   Vermeiden Sie es, Ihren kabellosen Router (oder Access Point) in der Nähe von Geräten, die radioaktive Strahlung abgeben (z. B. Mikrowellenherde), aufzustellen. Objekte, die die kabellose Kommunikation behindern können sind z.B.:

   - Kühlschränke
   - Waschmaschinen und/oder Wäschetrockner
   - Aktenschränke aus Metall
   - Große Aquarien
   - UV-Beschichtung von Fenstern auf Metallbasis

Wenn das Funksignal Ihrer kabellosen Verbindung an manchen Stellen schwach ist, sorgen Sie dafür, dass solche Objekte den Weg des Funksignals nicht blockieren (zwischen Ihren Computern und dem kabellosen Router oder Access Point).

3. **Schnurlose Telefone**

Wenn die Leistung Ihres kabellosen Netzwerks noch beeinträchtigt wird, nachdem Sie die oben genannten Hinweise beachtet und aber ein schnurloses Telefon haben:

- Versuchen Sie die schnurlosen Telefone aus der Nähe von kabellosen Routern (oder Access Points) und Ihren Computern, die für kabellose Vernetzung ausgerüstet sind, zu entfernen.
- Entfernen Sie die Batterie jedes schnurlosen Telefons, das im Frequenzband 2,4 GHz arbeitet, und ziehen Sie den Stecker am Anschluss heraus (Sehen Sie sich hierzu die Informationen des Herstellers an). Wenn das Problem dadurch behoben wird, ist Ihr Telefon möglicherweise der Auslöser der Störung.
- Wenn Sie Ihr Telefon über eine Kanalauswahl verfügt, wählen Sie einen Kanal für Ihr Telefon aus, der soweit wie möglich von dem Kanal Ihres kabellosen Netzwerks entfernt ist. Stellen Sie z. B. den Kanal Ihres Telefons auf 1 ein und den des kabellosen Routers oder Access Points auf 11. Mehr Informationen hierzu finden Sie im Benutzerhandbuch Ihres Telefons.
- Wenn es nötig ist, überlegen Sie sich, ein schnurloses Telefon anzuschaffen, das mit 900 MHz oder 5 GHz funktioniert.

4. **Wählen Sie den „ruhigsten” Kanal für Ihr kabelloses Netzwerk.**

An Orten, an denen es eine hohe Konzentration an Wohnräumen und Büros gibt, wie z.B. in Wohnblocks oder Bürogebäuden, kann Ihr kabelloses Netzwerk durch andere Netzwerke gestört werden.

Benutzen Sie die Standortübersicht (Site Survey) Ihres LAN-Programms für kabellose Netzwerke, um andere kabellose Netzwerke ausfindig zu machen, und stellen Sie Ihren kabellosen Router (oder Access Point) und Ihre Computer auf einen Kanal ein, der soweit wie möglich von den anderen Netzwerken entfernt ist.

Probieren Sie mehr als einen der möglichen Kanäle aus, um herauszufinden, welche Verbindung die beste ist und um Störungen durch schnurlose Telefone oder andere kabellose Geräte in der Umgebung zu vermeiden.

Wenn Sie kabellose Netzwerkprodukte von Belkin benutzen, verwenden Sie die detaillierte Standortübersicht (Site survey) und die Informationen über Kanäle für kabellose Geräte in Ihrem Benutzerhandbuch.

Diese Richtlinien sollten Ihnen helfen, den größtmöglichen Bereich mit Ihrem kabellosen Router (oder Access Point) abzudecken. Wenn Sie einen größeren Bereich abdecken müssen, empfehlen wir Ihnen den Kabellosen Range Extender/Access Point von Belkin.

5. Sichere Verbindungen, VPNs und AOL

Sichere Verbindungen sind Verbindungen, für die normalerweise ein Benutzername und ein Kennwort erforderlich ist. Sie werden überall benutzt, wo großer Wert auf Sicherheit gelegt wird. Zu sicheren Verbindungen zählen folgende:

- Virtual Private Network (VPN) Verbindungen, die oft benutzt werden, um auf Entfernung eine Verbindung mit einem Büronetzwerk herzustellen
- Das „Bring Your Own Access”-Programm von America Online (AOL), das Ihnen die Benutzung von AOL mit Breitband durch Kabel oder DSL-Service ermöglicht
- Die meisten Internetseiten für Bankangelegenheiten
- Viele kommerzielle Internetseiten, für die ein Benutzername und ein Kennwort erforderlich sind, um Ihnen Zugang zu Ihrem Konto zu verschaffen

Sichere Verbindungen können durch die Einstellung der Energieverwaltung (Power Management) eines Computers unterbrochen werden, die den „Ruhezustand” aktiviert. Die einfachste Möglichkeit, dies zu vermeiden, ist die Erstellung einer neuen Verbindung, indem Sie die VPN- oder AOL-Software neu starten oder sich wieder auf einer sicheren Internetseite einloggen.

Eine zweite Möglichkeit ist die Änderung der Einstellungen der Energieverwaltung, so dass der Ruhezustand deaktiviert ist; dies ist allerdings bei tragbaren Computern weniger angebracht. Wenn Sie die Einstellungen der Energieverwaltung unter Windows ändern wollen, sehen Sie in der Systemsteuerung unter „Power Options” (Energieoptionen) nach.

Wenn Sie weiterhin Probleme mit sicheren Verbindungen, VPNs oder AOL haben, beachten Sie bitte erneut die Schritte der vorherigen Seiten, um sicher zu stellen, dass Sie die angesprochenen Aspekte berücksichtigt haben.

Anhang C: Einstellungsübersicht für Internetverbindungen

Auf der nächsten Seite finden sie eine Übersicht mit möglichen Einstellungen Ihrer ADSL-Verbindung zum Auswählen und Einrichten einer Internetverbindung. Viele Internetprovider gebrauchen verschiedene Einstellungen, abhängig von der Region und der Ausstattung, die sie benutzen. Sie sollten die Einstellungen der Internetanbieter in Ihrer Region ausprobieren. Funktioniert dies nicht, fragen Sie bitte Ihren Internetprovider nach den benötigten Einstellungen.

Land	Verbindung-sprotokoll	VPI/VCI	Kapselung	ISPs (Internetprovider)
Europa				
Frankreich	PPPoE	8/35	LLC	Verschiedene
Deutschland	PPPoE	1/32	LLC	T-Online, verschiedene
Niederlande	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Verschiedene
Belgien	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italien	PPPoE oder PPPoA	8/35	VC MUX	TIN
Spanien	PPPoE oder 1483 Bridged	8/32	LLC	Telefonica
Schweden	1483 Bridged	3/35	LLC	Telia
GB	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Asien				
Australien	PPPoE oder PPPoA	8/35	LLC	Verschiedene
Neuseeland	PPPoE oder PPPoA	0/100	VC MUX	Verschiedene
Singapur	PPPoE	0/100	LLC	SingNet, Pacific Internet

FCC-Erklärung

KONFORMITÄTSERKLÄRUNG ZUR EINHALTUNG DER FCC-BESTIMMUNGEN ÜBER ELEKTROMAGNETISCHE KOMPATIBILITÄT

Wir, Belkin Corporation, eine Gesellschaft mit Sitz in 501 West Walnut Street, Compton, CA 90220, USA, erklären hiermit in alleiniger Verantwortung, dass dieser Artikel, Nr.

F5D9630-4

auf den sich diese Erklärung bezieht:
in Einklang mit Teil 15 der FCC-Regelungen steht. Der Betrieb unterliegt den beiden folgenden Bedingungen: (1) Dieses Gerät darf schädigende Störungen nicht verursachen, und (2) dieses Gerät muss jedwede Störung annehmen, einschließlich der Störungen, die einen unerwünschten Betrieb verursachen könnten.

Achtung: Hochfrequente Strahlungen.
Die Strahlungsleistung dieses Geräts liegt deutlich unter den FCC-Grenzwerten für hochfrequente Strahlungen. Dennoch ist bei der Gerätenutzung darauf zu achten, dass im Normalbetrieb Menschen möglichst wenig schädlichen Strahlungen ausgesetzt werden.

Beim Anschluss einer externen Antenne an das Gerät muss die Antenne so aufgestellt werden, dass im Normalbetrieb Menschen möglichst wenig mit schädlichen Strahlungen in Berührung kommen. Um sicherzustellen, dass die FCC-Grenzwerte für Belastungen durch hochfrequente Strahlungen nicht überschritten werden, ist im Normalbetrieb stets ein Abstand von mindestens 20 cm zur Antenne einzuhalten.

Hinweis der Federal Communications Commission
Dieses Gerät entspricht nachweislich den Grenzwerten für Digitalgeräte der Klasse B gemäß Abschnitt 15 der FCC-Bestimmungen. Diese Grenzwerte dienen dem angemessenen Schutz vor schädlicher Strahlung beim Betrieb von Geräten im Wohnbereich.

Das Gerät erzeugt und verwendet hochfrequente Strahlungen und kann sie ausstrahlen. Verursacht dieses Gerät Störungen des Radio- oder Fernsehempfangs (was sich durch Ein- und Ausschalten des Gerätes feststellen lässt), so können Sie versuchen, die Störung auf folgende Weise zu beseitigen:

- Andere Ausrichtung oder Standortänderung der Empfangsantenne
- Vergrößern des Abstands zwischen Gerät und Empfänger
- Anschluss des Geräts an eine Steckdose in einem anderen Stromkreis als dem des Empfängers
- Den Händler oder einen erfahrenen Rundfunk- und Fernsehtechniker hinzuziehen

Modifikationen
Nach den Vorschriften der FCC muss dem Benutzer mitgeteilt werden, dass Änderungen oder Modifikationen an diesem Gerät, die nicht ausdrücklich von der Belkin Corporation genehmigt wurden, dazu führen können, dass die Berechtigung des Benutzers zum Betrieb des Geräts erlischt.

Canada-Industry Canada (IC)
Das Funksystem dieses Geräts entspricht den Bestimmungen RSS 139 und RSS 210 von Industry Canada. Dieses digitale Gerät der Klasse B entspricht der kanadischen Norm ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Europa - Hinweis der europäischen Union
Die Kennzeichnung von Endeinrichtungen mit dem Zeichen CE 0560 oder dem CE-Symbol gibt an, dass das Gerät der Richtlinie (1995/5/EC) (R/TTE-Richtlinie) der EU-Kommission entspricht.

Aus einer solchen Kennzeichnung geht hervor, dass das Gerät den folgenden europäischen Normen entspricht (in Klammern die entsprechenden internationalen Standards):

- EN 60950 (IEC60950): Sicherheit von Einrichtungen der Informationstechnik
- EN 300 328 Technische Anforderungen an Funkgeräte
- ETS 300 826 Allgemeine Anforderungen zu elektromagnetischen Strahlungen von Funkgeräten

Den Sendertyp finden Sie auf dem Produkterkennungsschild Ihres Belkin-Produkts.

Produkte mit dem CE-Zeichen entsprechen der Richtlinie zur Elektromagnetischen Verträglichkeit (89/336/EWG) und der Niederspannungsrichtlinie (72/23/EWG) der EU-Kommission. Aus der Einhaltung dieser Richtlinien geht hervor, dass das Gerät den folgenden europäischen Normen entspricht (in Klammern die entsprechenden internationalen Standards).

- EN 55022 (CISPR 22): Funkstörungen
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Elektromagnetische Immunität
- EN 61000-3-2 (IEC610000-3-2) – Oberschwingungsströme
- EN 61000-3-3 (IEC610000-3-2) - Grenzwerte für Spannungsschwankungen und Flicker
- EN 60950 (IEC60950) - Sicherheit von Einrichtungen der Informationstechnik

Produkte mit diesem Sender werden mit dem CE 0560 oder CE-Hinweis versehen und sind ggf. auch mit dem CE-Zeichen gekennzeichnet.



Dieses Symbol auf dem dem Produkt oder dessen Verpackung gibt an, dass das Produkt nicht zusammen mit dem Restmüll entsorgt werden darf. Es obliegt daher Ihrer Verantwortung, das Gerät an einer entsprechenden Stelle für die Entsorgung oder Wiederverwertung von Elektrogeräten aller Art abzugeben (z. B. Wertstoffhof). Die separate Sammlung und das Recyceln Ihrer alten Geräte zum Zeitpunkt Ihrer Entsorgung trägt zum Schutz der Umwelt bei und gewährleistet, dass sie auf eine Art und Weise recycelt werden, die keine Gefährdung für die Gesundheit des Menschen und der Umwelt darstellt. Weitere Informationen darüber, wo Sie alte Elektrogeräte zum Recyceln abgeben können, erhalten Sie bei den örtlichen Behörden, Wertstoffhöfen oder dort, wo Sie das Gerät erworben haben.

Eingeschränkte lebenslange Produktgarantie von Belkin Corporation

Belkin Corporation gewährleistet hiermit, dass dieses Produkt während seiner gesamten Lebensdauer keine Verarbeitungs- und Materialfehler aufweisen wird. Bei Feststellung eines Fehlers wird Belkin das Produkt nach eigenem Ermessen entweder kostenlos reparieren oder austauschen, sofern es während des Garantiezeitraums ausreichend frankiert an den autorisierten Belkin-Händler zurückgegeben wurde, bei dem es erworben wurde. Ein Kaufnachweis kann verlangt werden.

Diese Garantie erstreckt sich nicht auf die Beschädigung des Produkts durch Unfall, missbräuchliche, unsachgemäße oder fehlerhafte Verwendung oder Anwendung. Ebenso ist die Garantie unwirksam, wenn das Produkt ohne schriftliche Genehmigung durch Belkin verändert oder wenn eine Belkin-Seriennummer entfernt oder unkenntlich gemacht wurde.

DIE VORSTEHENDEN GARANTIEBEDINGUNGEN UND RECHTSBEHELFE SCHLIESSEN ALLE ANDEREN GEWÄHRLEISTUNGEN UND RECHTSBEHELFE - OB MÜNDLICH ODER SCHRIFTLICH, AUSDRÜCKLICH ODER KONKLUDENT - AUS UND TRETEN AN DEREN STELLE. BELKIN ÜBERNIMMT INSBESONDERE KEINERLEI KONKLUDENTE GEWÄHRLEISTUNGEN, U.A. AUCH KEINE GEWÄHRLEISTUNG DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER HANDELSÜBLICHEN QUALITÄT.

Kein Händler, Bevollmächtigter bzw. Vertreter oder Mitarbeiter von Belkin ist befugt, diese Gewährleistungsregelung in irgendeiner Weise abzuändern oder zu ergänzen.

BELKIN HAFTET NICHT FÜR BESONDERE, DURCH ZUFALL EINGETRETENE ODER FOLGESCHÄDEN AUFGRUND DER VERLETZUNG EINER GEWÄHRLEISTUNG ODER NACH MASSGABE EINER ANDEREN RECHTSLEHRE (U.A. FÜR ENTGANGENE GEWINNE, AUSFALLZEITEN, GESCHÄFTS- ODER FIRMENWERTEINBUSSEN BZW. DIE BESCHÄDIGUNG, NEUPROGRAMMIERUNG ODER WIEDERHERSTELLUNG VON PROGRAMMEN ODER DATEN NACH SPEICHERUNG IN ODER NUTZUNG IN VERBINDUNG MIT BELKIN-PRODUKTEN).

Da in manchen Ländern der Ausschluss oder die Beschränkung der Haftung für durch Zufall eingetretene oder Folgeschäden bzw. ein Ausschluss konkludenter Gewährleistungen nicht zulässig ist, haben die vorstehenden Beschränkungen und Ausschlussregelungen für Sie möglicherweise keine Gültigkeit. Diese Garantie räumt Ihnen spezifische Rechte ein, die von Land zu Land unterschiedlich ausgestaltet sein können.

ADSL2+ Modem mit kabellosem G+ MIMO Router

Technische Informationen und Unterstützung erhalten Sie unter www.belkin.com im Bereich technischer Support.
“Wenn Sie den technischen Support telefonisch erreichen wollen, wählen Sie die entsprechende Nummer auf der unten aufgeführten Liste *.

*Zum normalen Telefontarif

Kostenloser technischer Support*

ÖSTERREICH	08 - 20 20 07 66	LUXEMBURG	34 20 80 8560
TSCHECHISCHE REPUBLIK	23 900 04 06	NIEDERLANDE	0900 - 040 07 90
DÄNEMARK	701 22 403	NORWEGEN	815 00 287
FINNLAND	00800 - 22 35 54 60	POLEN	00800 - 441 17 37
FRANKREICH	08 - 25 54 00 26	PORTUGAL	707 200 676
DEUTSCHLAND	0180 - 500 57 09	RUSSLAND	495 580 9541
GRIECHENLAND	00800 - 44 14 23 90	SÜDAFRIKA	0800 - 99 15 21
UNGARN	06 - 17 77 49 06	SPANIEN	902 - 02 43 66
ISLAND	800 8534	SCHWEDEN	07 - 71 40 04 53
IRLAND	0818 55 50 06	SCHWEIZ	08 - 48 00 02 19
ITALIEN	02 - 69 43 02 51	GROSSBRITANNIEN	0845 - 607 77 87

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220-5221, USA
310-898-1100
310-898-1111 Fax

Belkin Ltd.
7 Bowen Crescent, West Gosford
NSW 2250, Australien
+61 (0) 2 4372 8600
+61 (0) 2 4372 8603 Fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Großbritannien
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 Fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Niederlande
+31 (0) 20 654 7300
+31 (0) 20 654 7349 Fax

P75125ea_A

BELKIN

ADSL2+ modem met ingebouwde draadloze G+ MIMO router

Creëer een netwerk voor uw computers en deel uw ADSL-internetverbinding

UK
FR
DE
NL
ES
IT



Handleiding

802.11g
G+
MIMO

F5D9630df4A

Inhoud

Dank u voor het aanschaffen van dit ADSL-modem met ingebouwde hi-speed draadloze G router van Belkin (de router). Binnen een paar minuten kunt u uw internetaansluiting delen en vormen uw computers met uw nieuwe router een netwerk. Hier volgen enkele productkenmerken die deze router de ideale oplossing maken voor uw netwerk thuis of op kantoor. Wij raden u aan deze handleiding volledig door te lezen en extra aandacht te besteden aan Appendix B, getiteld “Belangrijke factoren die een rol spelen bij plaatsing en setup”.

Voordelen van een netwerk in uw woning

Als u de volgende eenvoudige setup-instructies volgt, kunt u met uw thuisnetwerk van Belkin het volgende doen:

- Uw hi-speed internetverbinding met alle computers in huis delen
- Bronnen als bestanden en harde schijven delen met alle aangesloten computers in huis
- Eén printer met het hele gezin delen
- Documenten, muziek, videomateriaal en digitale foto’s delen
- Bestanden opslaan, ophalen en kopiëren van de ene naar de andere computer
- Tegelijkertijd on-line spelletjes spelen, via het internet uw e-mail bekijken en chatten

Voordelen van een draadloos netwerk van Belkin

Mobiliteit – een speciale computerruimte is voortaan overbodig; u kunt nu overal binnen het draadloze bereik gebruik maken van een notebook of desktopcomputer die is aangesloten op het netwerk

Eenvoudige installatie – de Easy Installation Wizard van Belkin maakt installatie heel eenvoudig

Flexibiliteit – installatie van en toegang tot printers, computers en andere netwerkapparatuur vanaf elke plek in uw woning

Eenvoudige uitbreiding – Belkin biedt u keus uit een complete reeks netwerkproducten die het u mogelijk maken uw netwerk uit te breiden met apparaten als printers en gaming-consoles

Bedrading niet vereist – u bespaart uzelf de kosten en de moeite die komen kijken bij het aanleggen van Ethernet-kabels in uw woning of kantoor

Algemeen aanvaard – keuze uit een groot aanbod van interoperabele netwerkproducten

U dient over het volgende te beschikken

Inhoud van de verpakking

- ADSL2+ modem met ingebouwde draadloze G+ MIMO router
- RJ11-telefoonkabel - grijs
- RJ45 Ethernet-netwerkkabel - geel
- ADSL-microfilter*
- Voedingsadapter
- Handleiding (op cd)

*Benodigde ADSL-microfilters verschillen per land en worden niet in elk land meegeleverd. Als geen filter is meegeleverd, dient u er zelf een aan te schaffen.

Systeemvereisten

- Een actieve ADSL-lijn in combinatie met een telefoonaansluiting aan de muur, voor het aansluiten van de router
- Ten minste één computer met een netwerkinterfacekaart (NIC) en een internetbrowser die op de juiste wijze zijn geïnstalleerd en geconfigureerd
- TCP/IP-netwerkprotocol geïnstalleerd op alle computers die zijn aangesloten op de router
- Geen andere DHCP-server op uw lokale netwerk die IP-adressen aan computers en apparatuur toekent

Internetverbindingsinstellingen

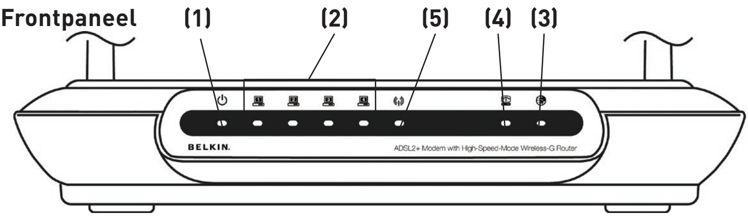
Vraag eerst uw Internet Service Provider (ISP) om de volgende informatie voordat u het draadloze ADSL-modem met ingebouwde draadloze G router installeert.

- Internetverbindingsprotocol: ________ (PPPoE, PPPoA, dynamisch IP, statisch IP)
- Multiplexing-methode of encapsulatie: __________ (LLC of VC MUX)
- Virtueel circuit: VPI (Virtual Path Identifier) __________ (een getal tussen 0 en 255)
- VCI (Virtual Channel Identifier) __________ (een getal tussen 1 en 65535)
- Voor PPPoE- en PPPoA-gebruikers: Gebruikersnaam _____________ en wachtwoord _______________ van uw ADSL-account
- Voor gebruikers van een statisch IP-adres IP Address ___ . ___ . ___ . ___
  Subnetmasker ___ . ___ . ___ . ___
  Standaard gatewayserver ___ . ___ . ___ .
- IP-adres voor Domain Name Server ___ . ___ . ___ . ___ (Indien verstrekt door uw ISP)

Let op: Zie Appendix C in deze handleiding voor enkele veelgebruikte DSL-parameters voor internetinstellingen. Bij twijfel raden wij u aan contact op te nemen met uw ISP.

De router is ontworpen voor plaatsing op een bureau. Met het oog op praktische bruikbaarheid lopen alle kabels via de achterzijde van de router naar uw apparatuur. De LED’s aan de bovenzijde van de router zijn goed zichtbaar en geven u informatie over de netwerkactiviteit en de status.

Frontpaneel



1. LED voor voeding

Als u de stroom naar de router (opnieuw) inschakelt, heeft de router enige tijd nodig om op te starten. Wanneer de router volledig is opgestart, brandt de LED voor voeding continu GROEN. Dit betekent dat de router klaar is voor gebruik.

	UIT	De router is UITgeschakeld
	Groen	De router is INgeschakeld
	Rood	De router kon niet opstarten

2. LAN status-LED’s

Deze LED’s zijn genummerd van 1 tot 4. Deze nummering correspondeert met de nummering van de poorten aan de achterkant van de router. De LED zal gaan branden als een computer correct wordt aangesloten op één van de LAN-poorten aan de achterkant van de router. Een GROENE LED die blijft branden houdt in dat er een apparaat is aangesloten dat geschikt is voor netwerkcommunicatie. Wanneer via de poort informatie wordt verzonden, knippert de LED snel. Een ORANJE LED geeft aan dat er sprake is van een 10Base-T-verbinding

	UIT	Er is geen apparaat aangesloten
	Oranje	Er is een Ethernet-verbinding tot stand gebracht en een 10Base-T-apparaat is aangesloten
	Oranje - knippert	Een 10Base-T-apparaat is bezig met het verzenden of ontvangen van gegevens
	Groen	Er is een Ethernet-verbinding tot stand gebracht en een 100Base-T-apparaat is aangesloten
	Groen - knippert	Een 100Base-T-apparaat is bezig met het verzenden of ontvangen van gegevens

3. WLAN status-LED

De status-LED voor WLAN brandt continu GROEN zodra draadloos LAN is geactiveerd. Hij knippert als de router bezig is met het draadloos versturen of ontvangen van gegevens.

	UIT	WLAN is uitgeschakeld
	Groen	WLAN-verbinding is tot stand gebracht
	Groen - knippert	Gegevens worden verstuurd of ontvangen

4. ADSL-LED

De ADSL-LED is GROEN en knippert tijdens de communicatie met uw ISP. Het lampje blijft GROEN branden als de router op de juiste manier met uw ADSL-service is verbonden.

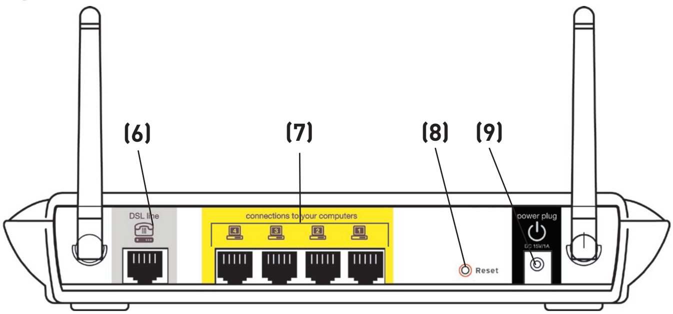
	UIT	Geen ADSL-verbinding
	Groen	ADSL-verbinding is tot stand gebracht
	Groen - knippert	Poging tot het maken van een verbinding

5. Internet-LED

De Internet-LED toont u wanneer de router een internetverbinding tot stand heeft gebracht. Wanneer de LED NIET brandt, is de router NIET verbonden met het Internet. Wanneer de LED continu GROEN licht geeft, is de router verbonden met het Internet. Als de LED knippert, is de router gegevens aan het ontvangen of versturen via het Internet.

	UIT	Geen internetverbinding
	Groen	Internetverbinding is tot stand gebracht
	Groen - knippert	Gegevens worden verstuurd of ontvangen
	Rood	Verkrijgen van IP mislukt

Achterpaneel



6. **DSL-lijn**
   Deze poort is voor het aansluiten van uw ADSL-lijn. Sluit uw ADSL-lijn aan op deze poort.
7. **Ethernet-poorten**
   De Ethernet-poorten zijn RJ45, 10/100 auto-negotiation-poorten. De poorten worden aangeduid met de cijfers 1 t/m 4. Deze cijfers corresponderen met genummerde LED's aan de voorkant van de router. Sluit de netwerkcomputers of andere netwerkapparatuur aan op deze poorten.
8. **Resetknop**
   De resetknop kan gebruikt worden in het zeldzame geval dat de router niet goed functioneert. Door de router te resetten, herstelt u de normale werking van de router terwijl de geprogrammeerde instellingen in behouden blijven. Met de resetknop kunt u ook de fabrieksinstellingen van het draadloze accesspoint terugroepen. U kunt de optie "Restore" (Herstellen) gebruiken wanneer u uw persoonlijke wachtwoord bent vergeten.
   a. **De router resetten**
      Druk de resetknop in en houd deze een seconde lang ingedrukt. Wanneer de LED voor "Voeding/Gereed" weer continu brandt, is de resetprocedure voltooid.
   b. **De standaard fabrieksinstellingen herstellen**
      Druk de resetknop gedurende vijf seconden in en laat hem daarna los. Wanneer de LED voor "Voeding/Gereed" weer continu brandt, zijn de fabrieksinstellingen hersteld.
9. **Voedingsaansluiting**
   Sluit de meegeleverde 15V-voedingsadapter aan op deze aansluiting. Als u het verkeerde type voedingsadapter gebruikt, kunt u uw router beschadigen.

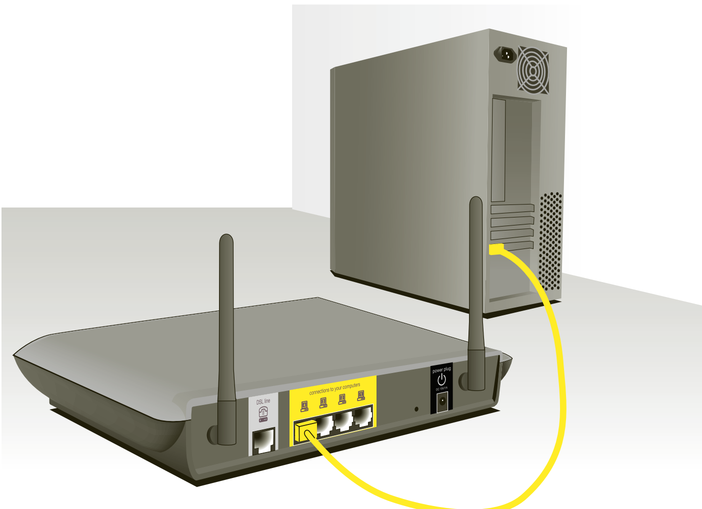
Kennismaken met uw router

Naarmate de afstand tussen de router en de computer kleiner is, wordt de verbinding sterker. Het bereik van draadloze apparatuur ligt doorgaans tussen de 30 en 60 meter. De prestaties van uw draadloze verbinding zullen iets achteruit gaan bij een grotere afstand tussen uw router en de aangesloten apparatuur. U hoeft hiervan niet altijd iets te merken. Bij een grotere afstand tot de router, kan de snelheid van de verbinding afnemen. Metalen apparaten of bloccades en muren kunnen signalen verzwakken doordat ze de radiogolven van uw netwerk blokkeren. Voor meer informatie verwijzen wij u naar “Appendix B: Belangrijke factoren die een rol spelen bij plaatsing en setup” in deze handleiding.

Als u denkt dat de matige prestaties van uw netwerk te maken hebben met afstand of hindernissen, probeer de computer dan op een afstand van 1,5 tot 3 meter van de router te plaatsen om te kijken of een te grote afstand inderdaad de oorzaak is. Als u zelfs problemen ondervindt bij zo’n korte afstand, raden wij u aan het hoofdstuk “Problemen oplossen” te raadplegen.

De computers aansluiten

1. Schakel uw computers en netwerkapparatuur uit.
2. Sluit uw computer met behulp van een Ethernet-netwerkkabel aan op een van de **GELE** RJ45-poorten, aangeduid met “connections to your computers” aan de achterzijde van de router (er is een Ethernet-netwerkkabel meegeleverd).



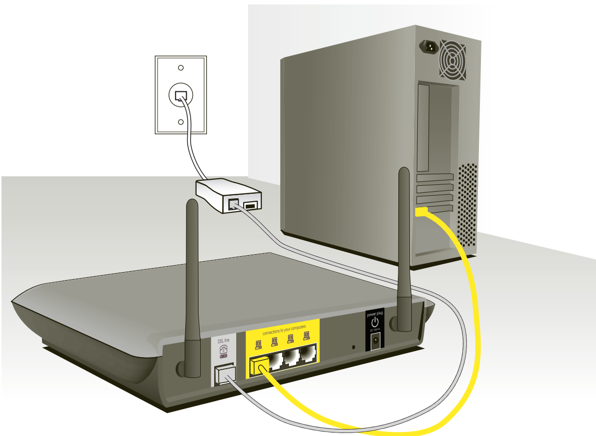
Uw router met de ADSL-lijn verbinden

De wijze waarop de router wordt aangesloten op de ADSl-lijn varieert per land en regio. Doorgaans heeft u een microfilter of een microfilter met ingebouwde splitter nodig om tegelijkertijd gebruik te kunnen maken van de ADSL-service en de telefoonservice op dezelfde telefoonlijn. Leest u de volgende stappen aandachtig door en maak uw keuze.

1. Indien uw telefoon- en ADSL-service van dezelfde telefoonlijn gebruik maken, zijn ADSL-microfilters nodig voor elke telefoon, fax, nummerherkenner of antwoordapparaat, etc. Extra splitters kunnen gebruikt worden voor het scheiden van telefoonlijnen voor gebruik voor de telefoon en de router.

   Let op: Sluit het ADSL-microfilter niet aan tussen de wandcontactdoos en de router— de ADSL-service kan anders namelijk niet bij het modem kunnen komen.

2. Indien uw telefoon- en ADSL-service van dezelfde telefoonlijn gebruik maken en u gebruik maakt van een ADSL-microfilter met ingebouwde splitter, sluit dan de splitter aan op de telefoonaansluiting aan de wand die de ADSL-service levert. Sluit vervolgens de telefoonkabel van de ADSL-microfilter RJ11-poort, doorgaans aangeduid met “DSL” aan op de grijze RJ11-poort aangeduid met “DSL line” op de achterzijde van de router. Sluit het telefoonapparaat aan op de andere poort van de ADSL-splitter, doorgaans aangeduid met “Phone”. U heeft een extra ADSL-microfilter als nog een telefoon of apparaat op dezelfde lijn is aangesloten.



Let op: Een RJ11-telefoonkabel is meegeleverd. Zorg er bij het bevestigen van een RJ11-stekker voor dat het lipje van de stekker op zijn plaats klikt.

3. Als u een speciale ADSL-service-telefoonlijn met een RJ11-aansluiting hebt, sluit dan eenvoudigweg een telefoonkabel aan tussen de aansluiting aan de wand en de grijze RJ11-poort die wordt aangeduid met “DSL line” aan de achterzijde van de router.

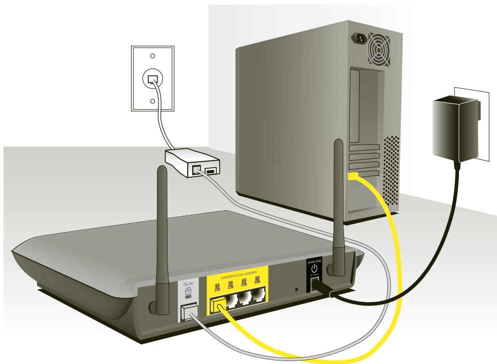
4. Als u een RJ45-aansluiting voor uw ADSL-service hebt, sluit dan een RJ45-naar-RJ11-converter aan op de wandaansluiting. Sluit vervolgens het ene uiteinde van een telefoonkabel aan op de converter en het andere uiteinde op de grijze RJ11-poort die wordt aangeduid met “DSL line” aan de achterzijde van de router.

Let op: Of de ADSL-microfilter is meegeleverd hangt af van het land van verkoop.

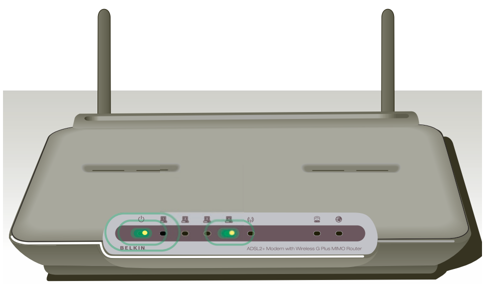
Uw router aanzetten

1. Sluit de meegeleverde voedingsadapter aan op de poort van de router die wordt aangeduid met “Power”.

   Let op: Voor uw veiligheid, voor optimale prestaties en om beschadiging van uw router te voorkomen, raden wij u aan uitsluitend de meegeleverde voedingsadapter te gebruiken.



2. Zodra u de voedingsadapter hebt aangesloten en de voedingsbron is ingeschakeld, zou het voedingspictogram ⏻ van de router op het frontpaneel ingeschakeld moeten zijn. Het kan enkele minuten duren voordat de router volledig is opgestart.



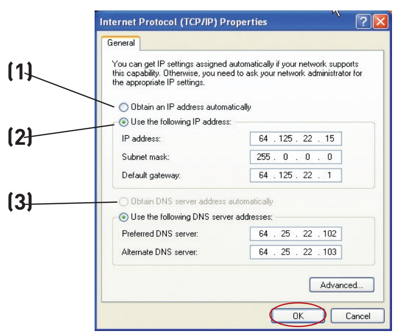
3. Zet uw computers aan. Nadat uw computers zijn opgestart, gaat aan de voorzijde van de router een LED voor de LAN-verbinding 💻 branden voor elke poort waarop een bedrade computer is aangesloten. Deze lampjes geven de status van de verbinding en activiteit weer. U kunt nu de router configureren voor een ADSL-verbinding.

Om ervoor te zorgen dat uw computer correct met uw router kan communiceren, dient u de “TCP/IP-Ethernet”-instellingen van uw computer te wijzigen in: “Obtain an IP address automatically/Using DHCP” (IP-adres automatisch ophalen/Gebruik maken van DHCP) Dit is de standaardinstelling voor de meeste homecomputers.

Installeer EERST de computer die is verbonden met het ADSL-modem. Volg daarbij de volgende stappen. U kunt deze stappen ook gebruiken om computers aan uw router toe te voegen nadat de router geconfigureerd is voor aansluiting op het Internet.

Handmatige configuratie van netwerkadapters onder WindowsXP, 2000 of NT

1. Klik op “Start”, “Settings” (Instellingen) en vervolgens op “Control Panel” (Configuratiescherm).
2. Dubbelklik op het pictogram “Network and dial-up connections” (Netwerk- en inbelverbindingen) (Windows 2000) of het pictogram “Network” (Netwerk) (Windows XP).
3. Klik met uw rechter muisknop op de “Local Area Connection” (Lokale verbinding) die is gekoppeld aan uw netwerkadapter en selecteer “Properties” (Eigenschappen) in het dropdown-menu.
4. Klik in het scherm “Local Area Connection Properties” (Eigenschappen lokale verbinding) op Internet Protocol (TCP/IP)” en vervolgens op de knop “Properties” (Eigenschappen). Nu verschijnt het volgende scherm:



5. Wanneer “Use the following IP address” (Gebruik het volgende IP-adres) **(2)** is geselecteerd, moet uw router worden geconfigureerd voor een verbinding met een statisch IP. Noteer de adresinformatie in de onderstaande tabel. U dient deze informatie in de router in te voeren.

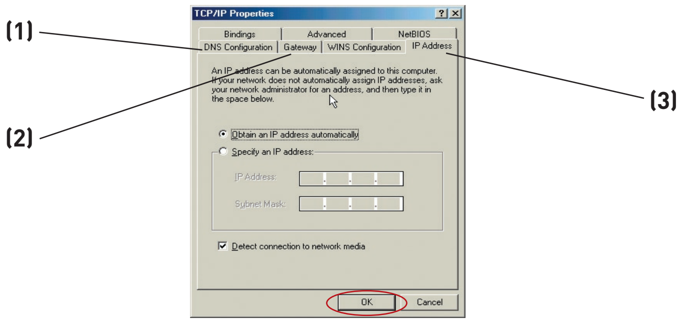
IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

6. Als dit niet al is geselecteerd, selecteer dan “Obtain an IP address automatically” (IP-adres automatisch ophalen) **(1)** en “Obtain DNS server address automatically” (DNS-serveradres automatisch ophalen) **(3)**. Klik op “OK”.

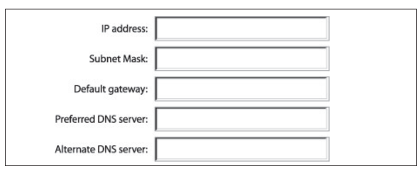
Uw netwerkadapter(s) is (/zijn) nu geconfigureerd voor gebruik met de router.

Handmatige configuratie van netwerkadapters onder Windows 98SE of Me

1. Klik in het dropdown-menu met uw rechter muisknop op “My Network Neighborhood” (Mijn netwerkomgeving) en selecteer “Properties” (Eigenschappen).
2. Selecteer “TCP/IP -> Settings” (TCP/IP -> Instellingen) voor de geïnstalleerde netwerkadapter. Het volgende venster zal verschijnen.



3. Als “Specify an IP address” (IP-adres specificeren) is geselecteerd, moet uw router worden geconfigureerd voor een verbinding met een statisch IP. Noteer de adresinformatie in de onderstaande tabel. U dient deze informatie in de router in te voeren.



4. Schrijf het IP-adres en subnetmasker over van het tabblad “IP Address” (IP-adres) **(3)**.
5. Selecteer het tabblad “Gateway” **(2)**. Vul het gatewayadres in het diagram in.
6. Selecteer het tabblad “DNS Configuration” (DNS-configuratie) **(1)**. Vul het DNS-adres/de DNS-adressen in het diagram in.
7. Als dit niet al is geselecteerd, selecteert u op het tabblad voor IP-adressen “Obtain IP address automatically” (IP-adres automatisch ophalen). Klik op “OK”.
8. Voor een correcte configuratie en verbinding met de router van Belkin dient u mogelijkerwijs ook de DNS-configuratiegegevens en het gateway-adres uit het gateway-tabblad te verwijderen.

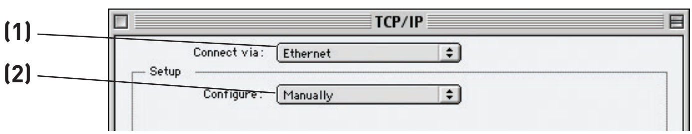
Start de computer opnieuw. Wanneer de computer opnieuw is opgestart, zijn uw netwerkadapters geconfigureerd voor gebruik met de router.

Installeer EERST de computer die is verbonden met het kabel- of DSL-modem. Volg daarbij de volgende stappen. U kunt deze stappen ook gebruiken om computers aan uw router toe te voegen nadat de router geconfigureerd is voor verbinding met het Internet.

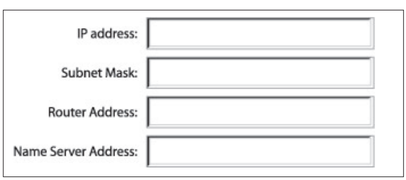
Handmatige configuratie van netwerkadapters onder Mac OS tot 9.x

Om ervoor te zorgen dat uw computer correct met uw router kan communiceren, dient u de TCP/IP-instellingen van uw Mac-computer in te stellen op DHCP.

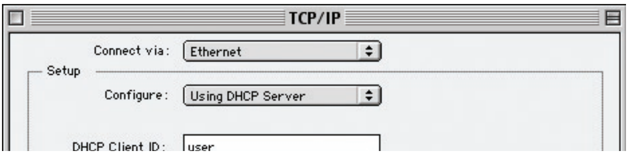
1. Open het “Apple”-dropdown-menu. Selecteer “Control Panels” (Configuratieschermen) en dan “TCP/IP”.
2. U ziet nu het TCP/IP-configuratiescherm. Selecteer “Ethernet Built-In” (Ethernet ingebouwd) of “Ethernet” in het dropdown-menu “Connect via:” (Verbinding maken via) **(1)**.



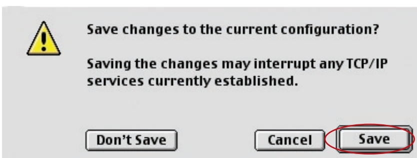
3. Als naast “Configure” (Configureren) **(2)**”Manually” (Handmatig) is geselecteerd, moet uw router ook worden geconfigureerd voor een verbinding met een statisch IP. Noteer de adresinformatie in de onderstaande tabel. U dient deze informatie in de router in te voeren.



4. Als dit niet al bij “Configure” (Configureren) is ingesteld, kiest u “Using DHCP Server”(Gebruik maken van DHCP-server). Hierdoor geeft u de computer de opdracht bij de router een IP-adres op te halen.



5. Sluit het venster. Als u veranderingen hebt aangebracht, verschijnt het volgende venster. Klik op “Save” (Opslaan).



Herstart de computer. Wanneer de computer opnieuw is opgestart, zijn uw netwerkinstellingen geconfigureerd voor gebruik met de router.

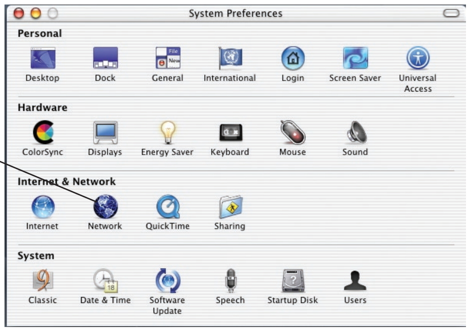
Netwerkadapters onder Mac OS X handmatig configureren

1. Klik op het pictogram “System Preferences” (Systeemvoorkeuren).



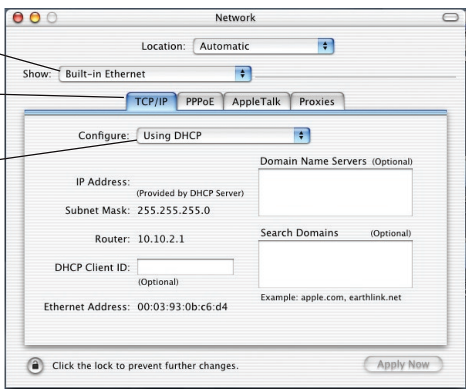
2. Selecteer “Network” (Netwerk) **(1)** in het menu “System Preferences” (Systeemvoorkeuren).

(1)



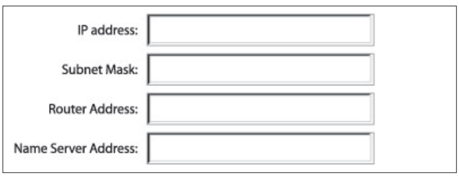
3. Selecteer “Built-in Ethernet” (Ingebouwd Ethernet) **(2)** naast “Show” (Tonen) in het netwerkmenu.

(2)
(3)
(4)



4. Selecteer het tabblad “TCP/IP” **(3)**. Naast “Configure” (Configureren)**(4)** moet nu “Manually” (Handmatig) of “Using DHCP” (Gebruikt maken van DHCP) te zien zijn. Is dat niet het geval, ga dan naar het tabblad PPPoE **(5)** en zorg ervoor dat “Connect using PPPoE” (Met behulp van PPPoE aansluiten) NIET is geselecteerd. Als dat wel het geval is, dan moet u uw router configureren voor een verbinding van het type PPPoE met behulp van uw gebruikersnaam en wachtwoord.

5. Als “Manually” (Handmatig) is geselecteerd, moet uw router worden geconfigureerd voor een verbinding met een statisch IP. Noteer de adresinformatie in de onderstaande tabel. U dient deze informatie in de router in te voeren.

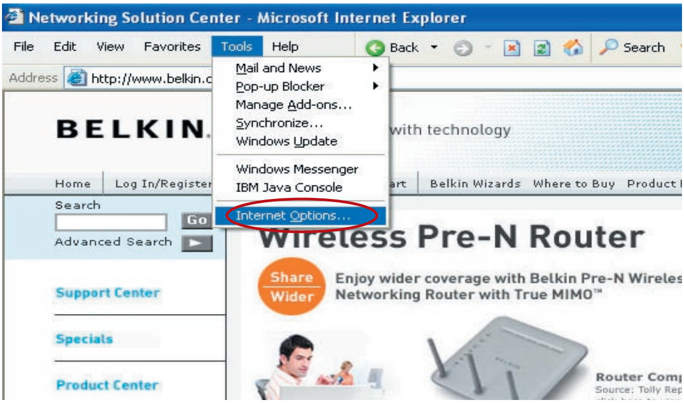


6. Als dit niet al is geselecteerd, selecteert u behalve “Configure” (Configureren) ook “Using DHCP” (Gebruik maken van DHCP) **(4)** en klikt u op “Apply Now” (Nu toepassen).

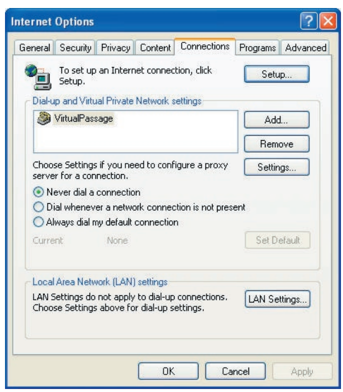
Uw netwerkadapter(s) is (/zijn) nu geconfigureerd voor gebruik met de router.

Aanbevolen instellingen van de webbrowser

Meestal hoeft u aan de instellingen van uw webbrowser niets te veranderen. Als u problemen hebt met het openen van het Internet of de geavanceerde via het Internet bereikbare gebruikersinterface, wijzig dan de huidige instellingen van uw browser in de aanbevolen instellingen die u in dit hoofdstuk vindt.

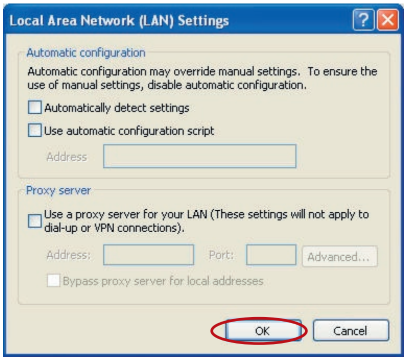


Internet Explorer 4.0 of hoger



1. Start uw browser. Selecteer "Tools" (Extra) en vervolgens "Internet Options" (Internetopties).
2. In het scherm "Internet Options" (Internetopties) vindt u drie keuzemogelijkheden. "Never dial a connection" (Nooit een verbinding maken), "Dial whenever a network connection is not present" (Maak verbinding indien er geen netwerkverbinding aanwezig is) en "Always dial my default connection" (Altijd mijn standaardverbinding gebruiken). Als u een keus kunt maken, selecteer dan "Never dial a connection" (Nooit een verbinding maken). Als u geen keus kunt maken, ga dan naar de volgende stap.
3. Klik op het scherm "Internetopties" op "Verbindingen" en selecteer "LAN-instellingen".

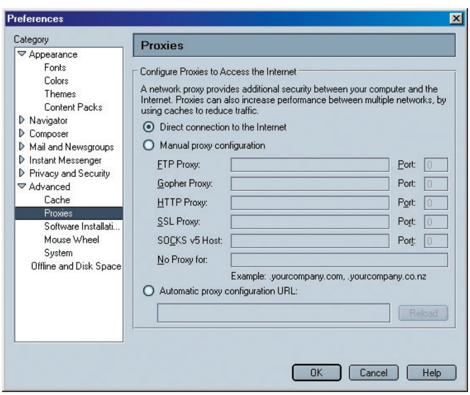
4. Zorg ervoor dat geen van de getoonde opties is aangevinkt: “Automatically detect settings” (Instellingen automatisch detecteren), “Use automatic configuration script” (Script voor automatische configuratie gebruiken) en “Use a proxy server” (Proxyserver gebruiken). Klik op “OK”. Klik vervolgens op de pagina “Internet Options” (Internetopties) opnieuw op “OK”.



Netscape Navigator 4.0 of hoger

1. Start Netscape. Klik op “Edit” (Bewerken) en vervolgens op “Preferences” (Voorkeurinstellingen).

2. Klik in het venster “Preferences” (Voorkeurinstellingen) op “Advanced” (Geavanceerd) en selecteer vervolgens “Proxies”. In het venster “Proxies” selecteert u “Direct connection to the Internet” (Rechtstreekse verbinding met het Internet).



Configuratie van de router met behulp van de Setup Wizard

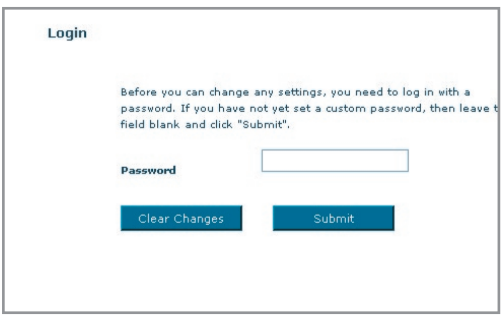
De Setup Wizard gebruiken

1. Op een computer die via kabels verbonden is met de router kunt u via de internetbrowser toegang krijgen tot de web-based gebruikersinterface van de router. Typ in de adresbalk van uw browser “192.168.2.1” in (zonder aanhalingstekens en zonder “http://” of “www” ervoor). Druk vervolgens op “Enter”.



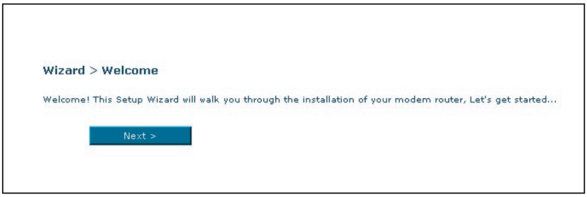
Let op: Wij raden u ten zeerste aan bij de eerste setup gebruik te maken van een computer die via een RJ45-kabel is aangesloten op de router. Gebruik maken van een computer die draadloos met de router is verbonden raden wij af.

2. Het volgende scherm zal verschijnen. Hierin wordt u verzocht in te loggen. De router wordt geleverd zonder vooraf geprogrammeerd wachtwoord. Laat het wachtwoord in het inlogscherm blanco en klik op de knop “Submit” (Verzenden) om in te loggen.

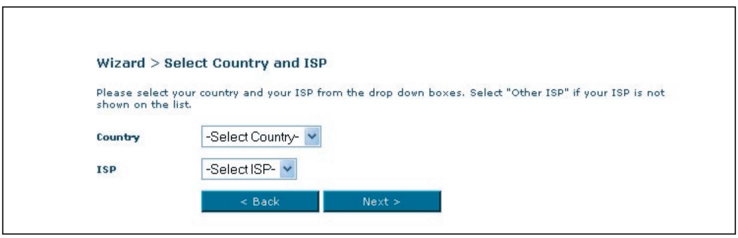


Let op: Wij raden u uit veiligheidsoverwegingen aan gebruik te maken van een wachtwoord. Gedetailleerde informatie over het wijzigen van een wachtwoord en over andere beveiligingsmogelij kheden vindt u in het hoofdstuk “Handmatige configuratie van de router”, in deze handleiding.

3. De Setup Wizard zal automatisch starten ten behoeve van een snelle configuratie (aanbevolen). Klik op “Next” (Volgende) om door te gaan.



4. De eerste stap is het selecteren van uw land en ISP. Vervolgens klikt u op “Next” (Volgende). Als uw land en/of ISP niet zijn opgenomen in het getoonde overzicht, selecteert u “Other Country” (Ander land) of “Other ISP” (Andere ISP)



5. Vul nu in het daarvoor bestemde veld de gebruikersnaam en het wachtwoord in dat u van uw Internet Service Provider (ISP) hebt gekregen. Het is belangrijk dat u de juiste informatie invult op de juiste plaats, anders zal er geen verbinding tot stand gebracht kunnen worden. Uw ISP zal uw gebruikersnaam en wachtwoord kunnen bevestigen.



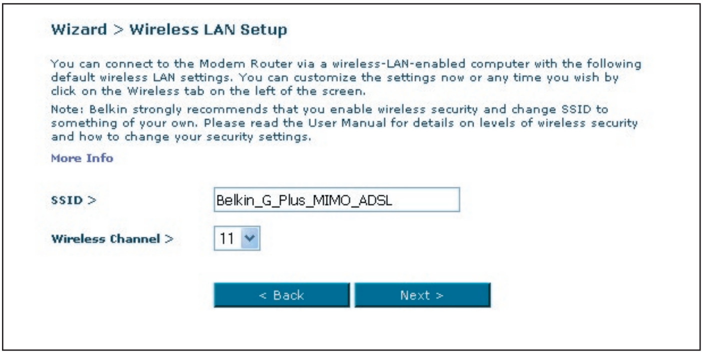
Let op: Voor meer gedetailleerde informatie over overige verbindingstypes, verwijzen wij u naar het hoofdstuk “Handmatige configuratie van de router”.

6. Het setup-scherm voor Wireless LAN (Draadloos LAN) zal verschijnen. U kunt nu verbinding maken met de router via een WLAN-computer met de volgende standaard instellingen voor draadloos LAN:

   SSID = Belkin G+ MIMO ADSL

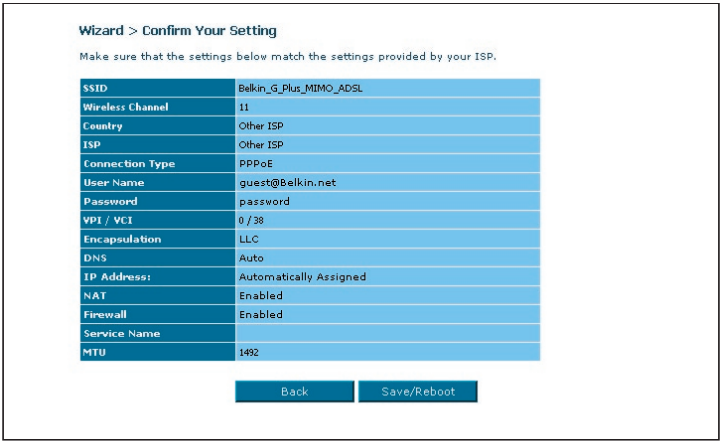
   Draadloos kanaal = Auto

   Beveiliging = off (uitgeschakeld)



Let op: Wij raden u aan gebruik te maken van beveiliging via WEP of WPA en de SSID een nieuwe naam te geven. Raadpleeg de handleiding voor meer informatie over beveiligingsniveaus voor draadloze netwerken en over het wijzigen van beveligingsinstellingen.

7. Controleer de instellingen die op het volgende scherm worden getoond. U kunt vervolgens klikken op de knop “Back” om de instellingen te wijzigen of op “Next” (Volgende) om te bevestigen.



Wizard > Confirm Your Setting

Make sure that the settings below match the settings provided by your ISP.

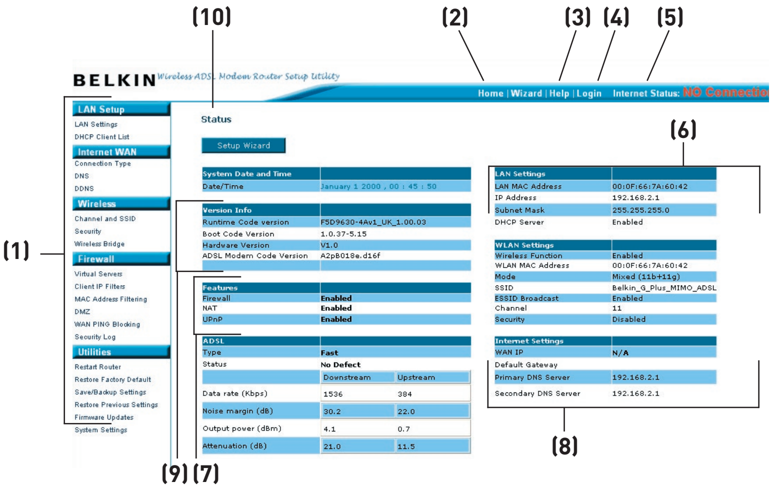
SSID	Belkin_G_Plus_MIMO_ADSL
Wireless Channel	11
Country	Other ISP
ISP	Other ISP
Connection Type	PPPoE
User Name	guest@Belkin.net
Password	password
VPI / VCI	0 / 38
Encapsulation	LLC
DNS	Auto
IP Address:	Automatically Assigned
NAT	Enabled
Firewall	Enabled
Service Name	
MTU	1492

Back   Save/Reboot

Let op: Voor het wijzigen van de gekozen instellingen kunt u de Setup Wizard herstarten of gebruik maken van het Navigatiemenu aan de linker zijde.

De werking van de geavanceerde web-based gebruikersinterface

Deze homepage geeft u een beknopt overzicht van de status en de instellingen van de router. Alle pagina’s voor geavanceerde installatie zijn vanaf deze pagina bereikbaar.



1. **Snelnavigatiekoppelingen**
U kunt rechtstreeks naar elke pagina van de gebruikersinterface van de router gaan door rechtstreeks op deze koppelingen te klikken. Om het opzoeken van een bepaalde instelling te vergemakkelijken, zijn de koppelingen onderverdeeld in logische categorieën en gegroepeerd op tabbladen. Als u klikt op de koptekst van een tabblad krijgt u een beknopte beschrijving van de functie van het tabblad.
2. **Home-knop**
De”Home”-knop is beschikbaar op elke pagina van de gebruikersinterface. Met een druk op deze knop gaat u terug naar de homepage.
3. **Help-knop**
Door middel van de helpknop kunt u de helppagina’s van de router openen. Met een klik op “More Info” (Meer informatie) kunt u op veel pagina’s naast bepaalde paragrafen ook om hulp vragen.
4. **Login/Logout-knop**
Met één druk op deze knop kunt u op de router in- en uitloggen. Wanneer u bent ingelogd, verandert de tekst op de knop in “Logout”.

Door op de router in te loggen, gaat u naar een afzonderlijke inlogpagina waar u een wachtwoord moet invoeren. Als u bent ingelogd, kunt u wijzigingen aanbrengen in de instellingen. Wanneer u klaar bent met het aanbrengen van wijzigingen, kunt u uitloggen door te klikken op de knop “Logout” (Afmelden). Meer informatie over inloggen op de router vindt u in het hoofdstuk “Inloggen op de router”.

5. **Internetstatusindicator**

Deze indicator is zichtbaar op alle pagina’s van de router en geeft de verbindingsstatus van de router weer. Wanneer de indicator met een GROEN lampje “Connection OK” (Verbinding OK) aangeeft, dan is er een verbinding met Internet tot stand gebracht. Wanneer de indicator met een rood lampje “No Connection” (Geen verbinding) aangeeft, is er geen verbinding met Internet tot stand gebracht. Deze indicator wordt automatisch bijgewerkt zodra u de instellingen van de router wijzigt.

6. **LAN-instellingen**

Toont u de instellingen van de Local Area Network (LAN) kant van de router. U kunt deze instellingen wijzigen door te klikken op de LAN-snelkoppeling aan de linkerzijde van het scherm.

7. **Features (Kenmerken)**

Hiermee wordt de status getoond van de UPnP, NAT, firewall-functies van de router. U kunt deze instellingen wijzigen door te klikken op een van de koppelingen of door te klikken op de snelnavigatiekoppelingen aan de linkerzijde van het scherm.

8. **Internetinstellingen**

Toont de instellingen van de internet/WAN-kant van de router die verbinding maakt met het Internet. U kunt deze instellingen wijzigen door te klikken op de “Internet/WAN”-snelnavigatiekoppeling aan de linkerzijde van het scherm.

9. **Versie-informatie**

Toont de firmwareversie, bootcode-versie, hardwareversie en het serienummer van de router.

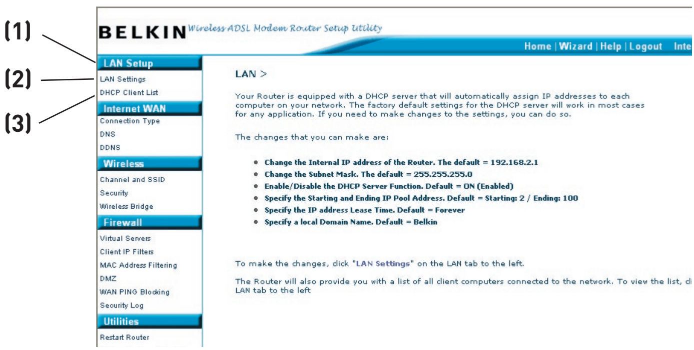
10. **Paginanaam**

De pagina waarop u zich bevindt, is herkenbaar aan deze naam. Deze handleiding verwijst soms naar de naam van de pagina’s. Bijvoorbeeld “LAN > LAN-instellingen” verwijst naar de pagina met “LAN-instellingen”.

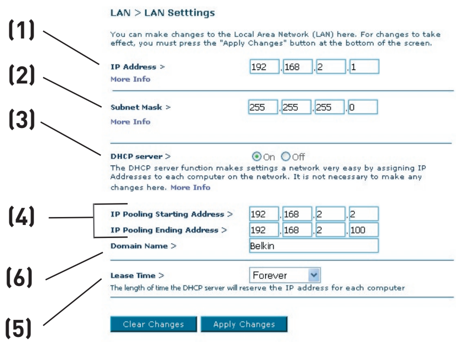
LAN-instellingen wijzigen

Hier kunt u alle instellingen van de interne LAN-setup van de router bekijken en aanpassen.

Als u klikt op de header van de LAN-tab **(1)** gaat u naar die pagina van de LAN-tab. Hier vindt u een beknopte beschrijving van de functies. Om de instellingen te bekijken of één van de LAN-instellingen te wijzigen, klikt u op “LAN Settings” (LAN-instellingen) **(2)** of als u een lijst wilt bekijken van de aangesloten computers, klikt u op “DHCP Client List” **(3)**.



LAN-instellingen



1. **IP-adres**

   Het “IP address” is het interne IP-adres van de router. Het standaard IP-adres is “192.168.2.1”. Om de geavanceerde setup-interface te openen, typt u het IP-adres in de adresbalk van uw browser in. U kunt dit adres indien nodig wijzigen. Om het IP-adres te wijzigen, typt u het nieuwe IP-adres in en klikt u op “Apply Changes” (Wijzigingen aanbrengen). Het IP-adres dat u kiest, moet een niet-routeerbaar IP zijn. Hieronder ziet u een paar voorbeelden van een niet-routeerbaar IP:

   192.168.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)

   10.x.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)

2. **Subnetmasker**

   Het subnetmasker hoeft niet gewijzigd te worden aangezien de router automatisch de lengte aanpast aan het type IP-adres.

3. **DHCP-server**

   De DHCP-serverfunctie maakt het installeren van een netwerk bijzonder gemakkelijk omdat aan elke computer in het netwerk automatisch een IP-adres wordt toegekend. De standaardinstelling is “On” (Ingeschakeld). U kunt deze instellingen wijzigen door te klikken op de “Internet/WAN”-snelnavigatiekoppeling aan de linkerzijde van het scherm. Om de DHCP-server uit te schakelen, selecteert u “Off” (Uitgeschakeld) en klikt u op “Apply Changes” (Wijzigingen aanbrengen).

4. **IP-pool**

   De IP-pool is de verzameling IP-adressen die gereserveerd is voor dynamische toewijzing aan de computers in uw netwerk. De standaardwaarde is 2-100 (99 computers). Als u dit aantal wilt veranderen, voert u een nieuw start- en

eind-IP-adres in en klikt u op “Apply Changes” (Wijzigingen aanbrengen). De DHCP-server kan honderd IP-adressen automatisch toewijzen. Dit betekent wel dat u geen IP-adressenpool kunt specificeren die groter is dan honderd computers. Als u bijvoorbeeld bij 50 begint, betekent dit dat u bij 150 of lager moet eindigen om de limiet van 100 cliënten niet te overschrijden. Het start-IP-adres moet altijd een lagere waarde hebben dan het eind-IP-adres.

5. **Leasetijd**

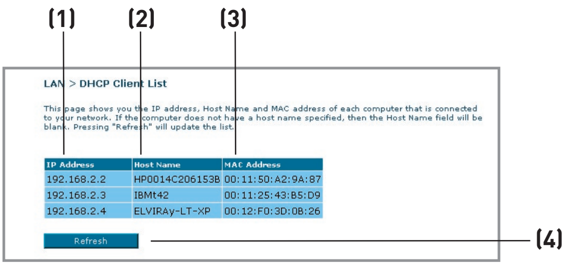
   De leasetijd is de periode die de DHCP-server het IP-adres voor elke computer bewaart. Het is beter dat de leasetijd ingesteld blijft op “Forever” (Altijd). Ook de standaard-instelling is “Forever” (Altijd). Dit betekent dat het door de DHCP-server aan een computer toegewezen IP-adres voor die bepaalde computer nooit verandert. Door het instellen van kortere leasetijden, zoals een dag of een uur, komen IP-adressen na de gespecificeerde tijdsduur vrij. Dit betekent ook dat het IP-adres van een bepaalde computer na verloop van tijd zou kunnen veranderen. Als u één van de andere geavanceerde functies van de router heeft ingesteld zoals DMZ of cliënt IP-filters, dan zijn deze afhankelijk van het IP-adres. Daarom is het niet waarschijnlijk dat u het IP-adres wilt wijzigen.

6. **Lokale domeinnaam**

   De standaardinstelling is “Belkin”. U kunt een lokale domeinnaam (netwerknaam) voor uw netwerk instellen. U hoeft deze instelling niet te wijzigen tenzij u daar een belangrijke reden voor hebt. U kunt het netwerk elke naam geven die u wilt zoals “MIJN NETWERK”.

DHCP-cliëntenlijst

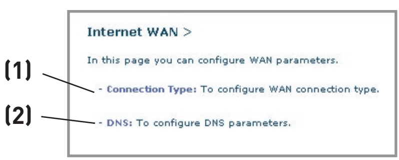
U kunt een overzicht bekijken van de computers (bekend als “clients” (cliënten)) die zijn aangesloten op uw netwerk. U kunt het IP-adres **(1)** van de computer bekijken, evenals de hostnaam **(2)** (als de computer er één heeft toegewezen gekregen) en het MAC-adres**(3)** van de computer’s netwerkinterfacekaart (NIC). Wanneer u de knop “Refresh” (Vernieuwen) **(4)** indrukt, wordt de lijst bijgewerkt. Als er dingen zijn gewijzigd, wordt de lijst bijgewerkt.



Internet WAN

Via de “Internet/WAN”-tab kunt u de router instellen voor het maken van verbinding met uw Internet Service Provider. De router kan met vrijwel elke ADSL-serviceprovider verbinding maken mits u de instellingen van de router hebt afgestemd op het type verbinding dat uw ISP gebruikt. Uw provider verstrekt u de benodigde gegevens. Om de router te configureren volgens de gegevens die uw ISP heeft verstrekt, klikt u op “Connection Type” (Verbindingstype) **(1)** links op het scherm. Selecteer het type verbinding dat u gebruikt. Als uw ISP u DNS-gegevens heeft gegeven, kunt u door op “DNS” **(2)** te klikken DNS-adresinformatie invoeren voor ISP’s die specifieke instellingen vereisen.

Als u klaar bent met het aanbrengen van instellingen, geeft de internetstatusindicator aan dat de verbinding in ordeis als uw router correct is geïnstalleerd.



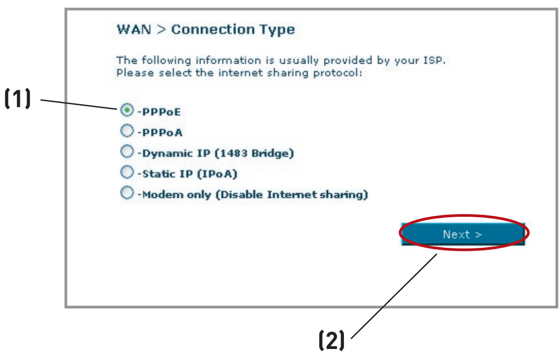
Verbindingstype

Op de pagina "Connection Type" (Type verbinding) kunt u een van deze vijf verbindingstypes selecteren, gebaseerd op de informatie die door verstrekt is door uw ISP.

- PPPoE
- PPPoA
- Dynamisch IP (1483 bridged)
- Statisch IP (IPOA)
- Modem Only (Disable Internet Sharing) ("Internetverbinding delen" uitschakelen)

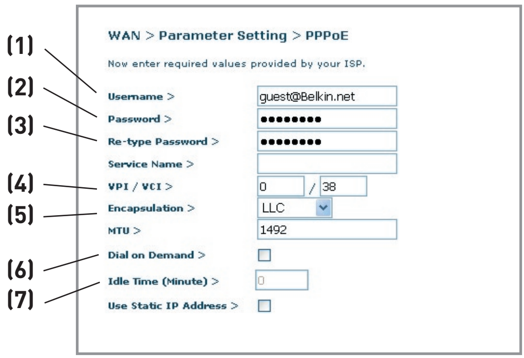
Let op: Zie Appendix C in deze handleiding voor enkele veelgebruikte DSL-parameters voor internetinstellingen. Bij twijfel raden wij u aan contact op te nemen met uw ISP.

Selecteer het type verbinding dat u gebruikt door op het keuzerondje **(1)** naast uw type verbinding te klikken en dan te klikken op "Next" (Volgende) **(2)**.



Uw ISP-verbindingstype instellen op PPPoE of PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) is de standaard methode voor het aansluiten van netwerkapparatuur. Een gebruikersnaam en wachtwoord zijn vereist om toegang tot het netwerk van uw ISP te verkrijgen en om een verbinding met Internet tot stand te kunnen brengen. PPPoA (PPP over ATM) is vergelijkbaar met PPPoE, maar wordt voornamelijk in het Verenigd Koninkrijk gebruikt. Selecteer PPPoE of PPPoA en klik op “Next” (Volgende). Voer vervolgens de informatie in die u van uw ISP gekregen hebt en klik op “Apply Changes” (Wijzigingen aanbrengen) om de instellingen te activeren.



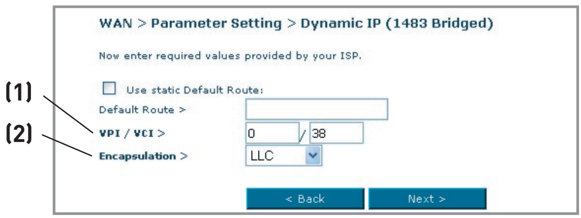
1. **Username (Gebruikersnaam) -** Typ de gebruikersnaam in. (Toegekend door uw ISP).
2. **Password (Wachtwoord) -** Vul uw wachtwoord in. (Toegekend door uw ISP).
3. **Retype Password (Wachtwoord opnieuw intypen) -** Bevestig uw wachtwoord. (Toegekend door uw ISP).
4. **VPI/VCI -** Vul uw Virtual Path Identifier (VPI) en Virtual Circuit Identifier (VCI) parameter hier in. (Toegekend door uw ISP).
5. **Encapsulation (Encapsulatie) -** Selecteer uw encapsulatietype (verstrekt door uw ISP) om aan te geven hoe meerdere protocols verwerkt moeten worden bij de ATM-transportlaag.

   VC-MUX: PPPoA Virtual Circuit Multiplexer (null encapsulation) laat slechts een protocol per virtual circuit toe, met minder overheads.

   LLC: PPPoA Logical Link Control staat meerdere protocols toe op een virtueel circuit (meer overhead).
6. **Dial on Demand -** Als u “Dial on Demand” selecteert, zal uw router automatisch verbinding maken met het Internet zodra een gebruiker de webbrowser opent.
7. **Idle Time (Minutes) -** Voer de maximale niet-actieve tijd in voor de Internet-verbinding. Nadat deze tijd is verstreken, zal de verbinding beëindigd worden.

Uw type internetverbinding instellen op Dynamic IP (1483 Bridged)

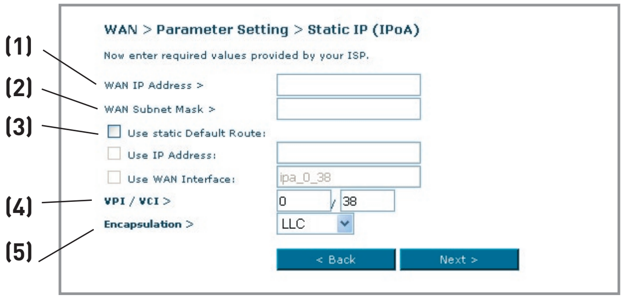
Deze verbindingsmethode zorgt voor een brug tussen uw netwerk en het netwerk van uw ISP. Aan de router zal automatisch een IP-adres worden toegekend door de DHCP-server van uw ISP.



1. **VPI/VCI -** Vul uw Virtual Path Identifier (VPI) en Virtual Circuit Identifier (VCI) parameter hier in. Deze gegevens worden verstrekt door uw ISP.
2. **Encapsulation (Encapsulatie) -** Selecteer LLC of VC MUX afhankelijk van wat uw ISP gebruikt.

Uw ISP-verbinding instellen op Static IP (IPoA)

Dit type verbinding wordt ook wel “Classical IP over ATM” of “CLIP” genoemd. Hierbij voorziet uw ISP u van een vast IP voor de verbinding van uw router met het Internet.



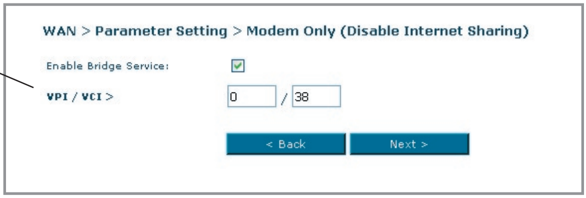
1. **WAN IP Address –** Vul het door uw ISP verstrekte IP-adres in voor de WAN-interface van de router.
2. **WAN Subnet Mask -** Vul het door uw ISP verstrekte subnetmasker in.
3. **Default Route -** Vul een standaard gateway IP-adres in. Indien de router binnen het lokale netwerk geen bestemmingsadres kan vinden, zal hij de pakketten doorsturen naar de standaard gateway die uw ISP heeft toegekend.
4. **VPI/VCI -** Vul uw Virtual Path Identifier (VPI) en Virtual Circuit Identifier (VCI) parameter hier in. Deze gegevens worden verstrekt door uw ISP.
5. **Encapsulation (Encapsulatie) -** Selecteer LLC of VC MUX afhankelijk van wat uw ISP gebruikt.

1
2
3
4
5
6
7
8
9
10
Hoofdstuk

Het verbindingstype instellen op Modem Only (Disable Internet Sharing) ("Internet delen" uitschakelen)

In deze modus fungeert de router uitsluitend als een bridge (brug) voor de overdracht van pakketten via de DSL-poort. Om een verbinding met het Internet tot stand te kunnen brengen, moet echter wel extra software op uw computer worden geïnstalleerd.

(1)

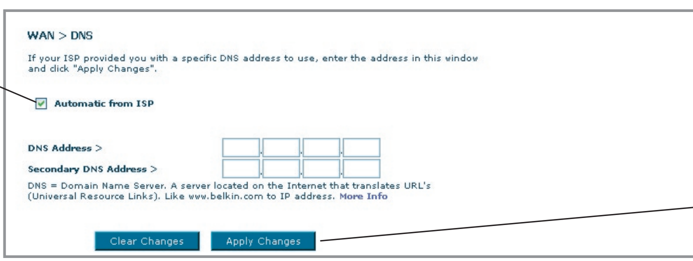


1. **VPI/VCI -** Vul uw Virtual Path Identifier (VPI) en Virtual Circuit Identifier (VCI) parameter hier in. (Toegekend door uw ISP).

Instellingen DNS (Domain Name Server)

Een "Domain Name Server" is een server op het Internet die URL's (Universal Resource Links) als "www.belkin.com" vertaalt in IP-adressen. De meeste ISP's verlangen niet van u dat u deze informatie in de router invoert. Het vakje "Automatic from ISP" (Automatisch van ISP) **(1)** moet zijn aangevinkt als uw ISP u geen specifiek DNS-adres heeft gegeven. Als u een statisch IP gebruikt, moet u waarschijnlijk een specifiek DNS-adres en een secundair DNS-adres invullen om ervoor te zorgen dat uw verbinding correct functioneert. Als u een dynamische verbinding of PPPoE gebruikt, hoeft u waarschijnlijk geen DNS-adres in te vullen. Laat het vakje behorend bij "Automatic from ISP" (Automatisch van ISP) aangevinkt. Om de gegevens van het DNS-adres in te voeren, verwijdert u het vinkje voor de optie "Automatic from ISP" en vult u uw DNS-gegevens in de daarvoor bestemde ruimte in. Klik op "Apply Changes" (Wijzigingen aanbrengen) **(2)** om de instellingen op te slaan.

(1)



(2)

Gebruik maken van een dynamisch DNS

De Dynamic DNS service staat statische hostnamen toe voor dynamische IP-adressen in een van de vele domeinen van DynDNS.org, waardoor toegang tot uw netwerkcomputers vanaf verschillende plaatsen op het internet eenvoudiger is. DynDNS.org biedt deze service, voor een maximum van vijf hostnamen, als een gratis dienst voor de internetgemeenschap.

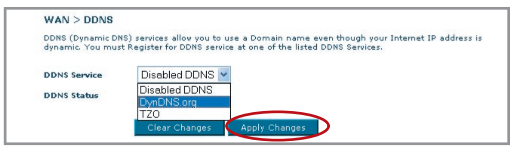
De dynamische DNS-service is ideaal voor een privé-website, bestandsserver, maar ook als u vanaf uw werk toegang wilt krijgen tot uw pc thuis en de bestanden die erop staan. Indien u gebruik maakt van deze service verzekert u zich ervan dat uw hostnaam altijd verwijst naar uw IP-adres, zelfs als uw ISP dit adres wijzigt. Indien uw IP-adres wijzigt, kunnen uw vrienden en zakenrelaties u altijd vinden via yourname.dyndns.org!

U kunt zich gratis aanmelden voor een Dynamische DNS-hostnaam via http://www.dyndns.org.

De Dynamic DNS Update Client van de router installeren.

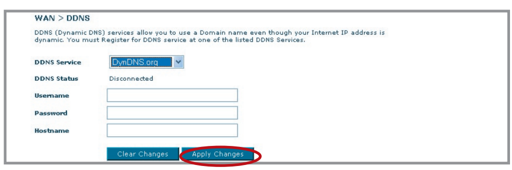
Voordat u van deze functionaliteit gebruik kunt maken, dient u zich aan te melden voor de gratis update-service van DynDNS.org. Zodra u dit gedaan hebt, kunt u verder. Volg daartoe onderstaande aanwijzingen.

1. Selecteer “DynDNS.org” in het dropdown-menu. Klik op “Apply Changes” (Wijzigingen aanbrengen).



2. Voer uw DynDNS.org-gebruikersnaam in in het veld “User Name” (Gebruikersnaam) **(1)**.
3. Voer uw DynDNS.org-wachtwoord in in het veld “Password / Key” **(2)**.
4. Voer de DynDNS.org domeinnaam die u met DynDNS.org hebt opgezet in in het veld “Domain Name” **(3)**.
5. Klik op “Apply Changes” (Wijzigingen aanbrengen) om uw IP-adres bij te werken.

Indien het door uw ISP aan u toegewezen IP-adres wijzigt, zal de router uw nieuwe IP-adres automatisch doorspelen aan de DynDNS.org-servers. U kunt dit ook handmatig doen door te klikken op de knop “Apply Changes” (Wijzigingen aanbrengen) **(4)**.



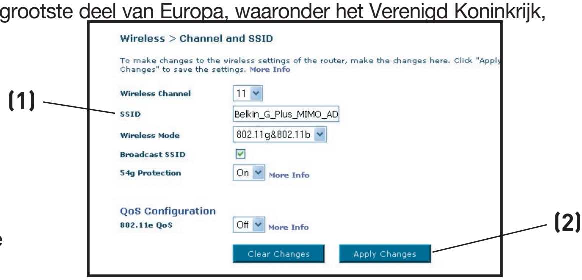
Het Wireless-tabblad

Op het tabblad “Wireless” (Draadloos) kunt u veranderingen aanbrengen in de instellingen van het draadloze netwerk. Op dit tabblad kunt u de naam van het draadloze netwerk (SSID), het gebruikte kanaal en de encryptie-instellingen aanpassen.

Kanaal en SSID

1. Het draadloze kanaal wijzigen

U kunt kiezen uit verschillende kanalen. In de Verenigde Staten zijn 11 kanalen beschikbaar. In het grootste deel van Europa, waaronder het Verenigd Koninkrijk, zijn 13 kanalen beschikbaar. Een klein aantal andere landen stelt andere eisen aan het kanaalgebruik. Uw router is zo ingesteld dat hij actief kan zijn op de juiste kanalen voor het land waarin u zich bevindt. Het standaard kanaal is 11 (behalve als u zich in een land bevindt waarin kanaal 11 niet gebruikt mag worden). Indien nodig kan dit adres worden gewijzigd. Als er meer draadloze netwerken in uw gebied actief zijn, moet uw netwerk op een ander kanaal worden ingesteld dan de andere draadloze netwerken. U bereikt het beste resultaat door een kanaal te kiezen dat minstens vijf kanalen verwijderd is van andere draadloze netwerken. Als een ander netwerk bijvoorbeeld kanaal 11 gebruikt, stel uw netwerk dan in op kanaal 6 of lager. Om het kanaal te veranderen, kiest u een kanaal in het dropdown-menu. Klik op “Apply Changes” (Wijzigingen aanbrengen). De wijziging is onmiddellijk van kracht.



2. De naam van het draadloze netwerk (SSID) wijzigen

Om uw draadloze netwerk te identificeren, wordt een naam gebruikt die bekend is als SSID (Service Set Identifier). De standaard SSID van de router is “belkin54g”. U kunt deze naam veranderen in alles wat u maar wilt of u kunt hem onveranderd laten. Als er andere draadloze netwerken in uw omgeving actief zijn, stelt u het waarschijnlijk op prijs dat uw SSID uniek is (dus niet hetzelfde is als die van een ander draadloos netwerk in uw omgeving). Als u de SSID wil veranderen, typ dan de SSID die u wilt gebruiken in het SSID-veld in**(1)** en klik op “Apply Changes” (Wijzigingen aanbrengen)**(2)**. De verandering gaat onmiddellijk in. Als u de SSID verandert, moeten ook uw draadloos werkende computers opnieuw worden geconfigureerd om verbinding te kunnen maken met uw nieuwe netwerknaam. Zie de handleiding van uw draadloze netwerkadapter voor informatie over hoe u deze verandering moet aanbrengen.

3. Gebruik maken van de ESSID Broadcast-functie

Om veiligheidsredenen kunt u ervoor kiezen de SSID van uw netwerk niet uit te zenden. Daardoor blijft de naam van uw netwerk verborgen voor computers die de ether aftasten naar de aanwezigheid van draadloze netwerken. Om de uitzending van uw SSID stop te zetten, dient u het vinkje te verwijderen uit het vakje naast de optie Broadcast SSID. De verandering gaat onmiddellijk in. Elke computer moet nu worden ingesteld op het maken van verbinding met uw specifieke SSID; een SSID in de vorm van “ANY” (Elke) wordt niet langer geaccepteerd. Zie de handleiding van uw draadloze netwerkadapter voor meer informatie over hoe u deze verandering moet aanbrengen.

Let op: Deze geavanceerde functie mag uitsluitend door ervaren gebruikers worden toegepast.

4. De draadloze modus instellen

Uw router kan in twee verschillende draadloze modi werken:

- **802.11b & 802.11g-** Selecteer deze optie als u van plan bent zowel draadloze 802.11b- als 802.11g-cliënten binnen uw netwerk te gebruiken.
- **802.11g -** Gebruik deze modus als u geen gebruik maakt van 802.11b-cliënten binnen uw netwerk. Deze optie zorgt voor de beste netwerkprestaties, maar staat u niet toe 802.11b-cliënten op uw netwerk aan te sluiten.

5. Protected Mode-schakelaar

Als onderdeel van de 802.11g-specificatie garandeert de Protected-modus een goede werking van de 802.11g-cliënten en accesspoints als er veel 802.11b-verkeer is in de bedrijfsomgeving. Als de Protected-modus is INgeschakeld, scant 802.11g naar ander draadloos netwerkverkeer voordat hij gegevens verzendt. Daarom levert deze modus de beste prestaties in omgevingen met veel 802.11b-verkeer of interferentie. Als u zich in een omgeving bevindt met zeer weinig of geen draadloos netwerkverkeer, worden de beste prestaties geleverd als de Protected-modus is uitgeschakeld.

Encryptie/Beveiliging:

Het WiFi-netwerk beveiligen

Hier volgen een aantal manieren om de beveiliging van uw draadloze netwerk te verbeteren en uw data voor nieuwsgierige ogen en oren af te schermen. Dit overzicht is van toepassing voor de privé- of kleinzakelijke gebruiker. Op het moment van publicatie van deze handleiding, zijn er drie encryptiemethoden beschikbaar.

Naam	64-Bit Wired Equivalent Privacy	128-Bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acro-niem	64-bit WEP	128-bit WEP	WPA-TKIP/AES (of alleen WPA)	WPA2-AES (of alleen WPA2)
Beveilig-ing	Goed	Beter	Uitstekend	Uitstekend
Product-ken-merken	Statische sleu-tels	Statische sleu-tels	Dynamische encryptiesleutels en tweezijdige authentificatie	Dynamische encryptiesleutels en tweezijdige authentificatie
	Encryptiesleutels gebaseerd op het RC4-algorit-me (meestal 40-bits sleutels)	Veiliger dan 64-bits WEP-encryptie met een sleutellengte van 104 bits plus 24 extra bits van door het sys-teem gegener-eerde data.	TKIP (Temporal Key Integrity Protocol); ter verhoging van de veiligheid worden de sleutels continu gewijzigd	AES (Advanced Encryption Stan-dard) beveiligt zonder snel-heidsverlies

WEP (Wired Equivalent Privacy)

WEP is een protocol dat beveiliging van draadloze producten die voldoen aan de WiFi-standaard mogelijk maakt. WEP werd ontwikkeld om draadloze netwerken dezelfde mate van privacybescherming te bieden als vergelijkbare bekabelde netwerken.

64-bits WEP

64-bits WEP werd als eerste geïntroduceerd met 64-bits encryptie, bestaande uit een sleutel met een lengte van 40 bits plus 24 extra bits van door het systeem gegenereerde data (totaal 64 bits). Er zijn hardwarefabrikanten die 64-bits echter 40-bits encryptie noemen. Kort na de introductie van deze technologie ontdekten onderzoekers dat 64-bits encryptie te eenvoudig te decoderen was.

128-bits WEP

Aangezien beveiliging via 64-bits WEP-encryptie mogelijkerwijs niet toereikend zou zijn, werd een veiligere methode ontwikkeld, namelijk 128-bits WEP-encryptie. De 128-bits encryptie is opgebouwd uit een sleutellengte van 104 bits plus 24 extra bits van door het systeem gegenereerde data (128 bits in totaal). Er zijn hardwarefabrikanten die 128-bits echter 104-bits encryptie noemen.

De meeste nieuwe draadloze apparatuur die momenteel op de markt is, ondersteunt zowel 64-bits als 128-bits WEP-encryptie wat niet uitsluit dat u oudere apparatuur bezit die alleen 64-bits WEP-encryptie ondersteunt. Alle draadloze apparatuur van Belkin ondersteunt zowel 64-bits als 128-bits WEP-encryptie.

Encryptiesleutels

Nadat u de 64-bits of 128-bits WEP-encryptiemodus hebt gekozen, dient u een encryptiesleutel te genereren. Als de encryptiesleutel niet consequent in uw gehele draadloze netwerk gebruikt wordt, kunnen de op het netwerk aangesloten apparaten niet goed met elkaar communiceren.

U kunt de sleutel invoeren door de hexadecimale sleutel handmatig in te typen of u kunt een “Passphrase” (Meervoudig wachtwoord) intypen in het daarvoor bestemde veld en klikken op “Generate” (Genereren) om een sleutel te maken. Een hexadecimale sleutel is een combinatie van cijfers en letters van A tot F en 0 tot 9. Voor 64-bits WEP-encryptie dient u 10 hexadecimale tekens in te voeren. Voor 128-bits WEP-encryptie dient u 26 hexadecimale tekens in te voeren.

Een WEP-passphrase (samengesteld wachtwoord) is NIET hetzelfde als een WEP-sleutel. Uw draadloze netwerkkaart gebruikt deze passphrase om uw WEP-sleutels te genereren, maar de methode voor het aanmaken van sleutels verschilt per hardwarefabrikant. Als uw netwerk uit apparaten van verschillende leveranciers is opgebouwd, kunt u het beste de hexadecimale WEP-sleutel van uw router of accesspoint aanhouden en deze met de hand invoeren in de tabel voor de hexadecimale WEP-sleutel in het configuratiescherm van uw draadloze kaart.

Gebruik maken van een hexadecimale sleutel

Een hexadecimale sleutel is een combinatie van cijfers en letters van A t/m F en van 0 t/m 9. 64-bits sleutels bestaan uit vijf tweecijferige getallen. 128-bits sleutels zijn opgebouwd uit dertien paren van 2 tekens.

Bijvoorbeeld:
AF 0F 4B C3 D4 = 64-bits sleutel
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bits sleutel

Stel in de onderstaande vakken uw sleutel samen door in elk vakje twee tekens in te vullen. U kunt hierbij gebruik maken van de letters A t/m F en de cijfers 0 t/m 9. U gebruikt deze sleutel om de encryptie-instellingen te bepalen voor uw router en de op uw draadloze netwerk aangesloten computers aangesloten op uw draadloze netwerk.

Opmerking voor Mac-gebruikers: De oorspronkelijke Apple AirPort®-producten ondersteunen uitsluitend 64-bits encryptie. Apple AirPort 2-producten kunnen 64-bits en 128-bits encryptie ondersteunen. Controleer dus eerst welk type apparaat u gebruikt. Als het u niet lukt uw netwerk met 128-bits encryptie te configureren, probeer dan 64-bits encryptie.

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) is een nieuwe WiFi-standaard die een betere beveiliging biedt dan WEP-encryptie. De stuurprogramma's en software van uw draadloze apparatuur ondersteunen WPA slechts na een upgrade. Updates kunt u vinden op de website van de leverancier van uw draadloze product. Er zijn twee soorten WPA-beveiliging: WPA-Personal (PSK) en WPA-Enterprise (RADIUS).

WPA-Personal (PSK)

Deze methode maakt gebruik van een zogenaamde Pre-Shared key als netwerksleutel. Een netwerksleutel is een wachtwoord dat tussen de 8 en 63 tekens lang is. Dit wachtwoord kan zijn opgebouwd uit een combinatie van letters, cijfers en andere tekens. Elke cliënt maakt gebruik van dezelfde netwerksleutel om toegang te krijgen tot het netwerk. Dit is de modus die meestal in huiselijke omgeving wordt gebruikt.

WPA-Enterprise (RADIUS)

Bij dit systeem wordt er door een radiusserver automatisch een netwerksleutel aan de clienten toegekend. Van deze modus wordt doorgaans in kantoren en bedrijven gebruik gemaakt. Ga voor een overzicht van de draadloze producten van Belkin die WPA ondersteunen naar onze website: **www.belkin.com/networking**.

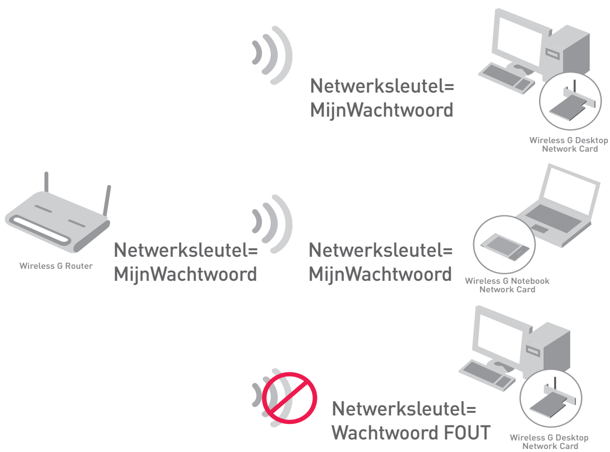
WPA2 (WiFi Protected Access)

WPA2 is de tweede generatie WPA die gebaseerd is op de 802.11i-standaard en maakt een betere beveiliging van uw draadloze netwerk mogelijk doordat geavanceerde netwerkauthentificatie en een complexere AES encryptietechniek gecombineerd worden. Net als WPA-beveiliging is WPA2 beschikbaar in WPA2-Personal (PSK) modus en WPA2-Enterprise (RADIUS) modus. WPA2-Personal (PSK) is de modus die doorgaans gebruikt worddt in een woonomgeving terwijl WPA-Enterprise (RADIUS) doorgaans wordt geïmplementeerd in werkomgevingen waarin een externe radiusserver de netwerksleutel automatisch distribueert naar alle cliënten.

Netwerksleutels delen

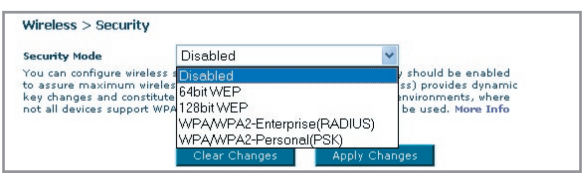
De meeste Wi-Fi-producten worden geleverd met uitgeschakelde beveiliging. Dus zodra u uw netwerk hebt geïnstalleerd, dient u WEP-encryptie, WPA of WPA2 te activeren en te zorgen dat al uw draadloze apparatuur dezelfde netwerksleutel delen.

De draadloze G+ MIMO desktopkaart biedt geen toegang tot het netwerk omdat deze een andere netwerksleutel gebruikt dan de netwerksleutel die is geconfigureerd in de draadloze G+ MIMO router.



Instellingen voor beveiliging van uw draadloze netwerk wijzigen

Uw router is uitgerust met WPA/WPA2 (Wi-Fi Protected Access), de nieuwste beveiligingsstandaard voor draadloos netwerkverkeer. Tevens wordt WEP (Wired Equivalent Privacy)-beveiliging ondersteund. Normaal is de beveiliging van een draadloos netwerk uitgeschakeld. Om beveiliging mogelijk te maken, dient u eerst te bepalen welke standaardinstelling u wilt gebruiken. Om de beveiling ingsinstellingen te wijzigen, klikt u op “Security” (Beveiliging) op het tabblad “Wireless” (Draadloos).



1
2
3
4
5
6
7
8
9
10
Hoofdstuk

WEP-setup

64-bits WEP-encryptie

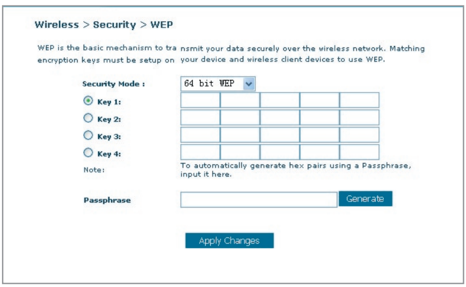
1. Selecteer “64-bit WEP” in het dropdown-menu.

2. Nadat u de WEP-encryptiemodus hebt geselecteerd, kunt u uw sleutel invoeren door de hexadecimale sleutel handmatig in te typen.

Een hexadecimale sleutel bestaat uit een combinatie van cijfers en letters van A tot F en van 0 tot 9. Voor 64-bits WEP-encryptie dient u 10 hexadecimale tekens in te voeren.

Bijvoorbeeld:

AF 0F 4B C3 D4 = 64-bits WEP-sleutel



3. Klik op “Apply Changes” (Wijzigingen aanbrengen) om te eindigen. De encryptie in de router is nu ingesteld. Iedere computer binnen uw draadloze netwerk moet nu worden geconfigureerd met dezelfde beveiligingsinstellingen..

WAARSCHUWING: Als u de draadloze router of het draadloze accesspoint vanaf een computer met een draadloze cliënt configureert, dient u ervoor te zorgen dat de beveiliging voor die draadloze cliënt is ingeschakeld, anders wordt de verbinding verbroken. Zorg ervoor dat u de sleutel ergens noteert voordat u de wijzigingen aanbrengt.

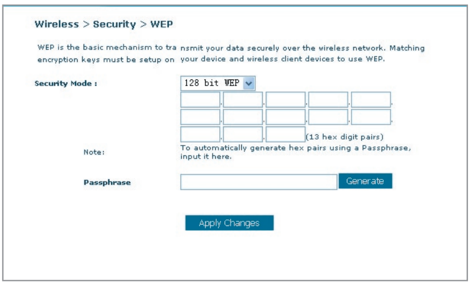
128-bits WEP-encryptie

1. Selecteer “128-bit WEP” in het dropdown-menu.
2. Nadat u de WEP-encryptiemodus hebt geselecteerd, kunt u uw sleutel invoeren door de hexadecimale sleutel handmatig in te typen.

   Een hexadecimale sleutel bestaat uit een combinatie van cijfers en letters van A tot F en van 0 tot 9. Voor 128-bits WEP-encryptie dient u 26 hexadecimale tekens in te voeren.

   Bijvoorbeeld:

   C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bits WEP-sleutel



3. Klik op “Apply Changes” (Wijzigingen aanbrengen) om te eindigen. De encryptie in de router is nu ingesteld. Iedere computer binnen uw draadloze netwerk moet nu worden geconfigureerd met dezelfde beveiligingsinstellingen.

WAARSCHUWING: Als u de draadloze router of het draadloze accesspoint vanaf een computer met een draadloze cliënt configureert, dient u ervoor te zorgen dat de beveiliging voor die draadloze cliënt is ingeschakeld, anders wordt de verbinding verbroken. Zorg ervoor dat u de sleutel ergens noteert voordat u de wijzigingen aanbrengt.

WPA-setup

Let op: Om WPA-beveiliging te kunnen gebruiken moeten al uw cliënten geüpgraded zijn naar stuurprogramma’s en software die WPA ondersteunen. U kunt ook gratis een beveiligingspatch van Microsoft downloaden. Deze patch werkt alleen onder het Windows XP-besturingssysteem. U dient tevens van de website van Belkin het nieuwste stuurprogramma te downloaden voor uw draadloze G desktop- of notebooknetwerkkaart. Andere besturingssystemen worden op dit moment nog niet ondersteund. De patch

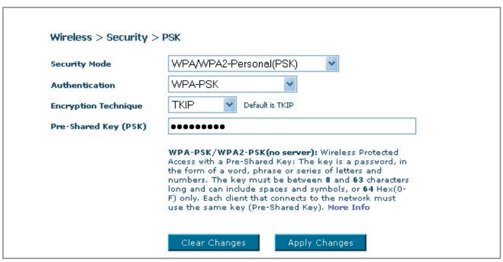
van Microsoft ondersteunt uitsluitend apparaten zoals 802.11g-producten van Belkin met stuurprogramma's die WPA ondersteunen.

Er zijn twee soorten WPA-beveiliging: WPA-Personal (PSK) en WPA-Enterprise (RADIUS). WPA-Personal (PSK) gebruikt een zogenaamde "Pre-Shared Key" als beveiligingssleutel. Een Pre-Shared Key is een wachtwoord dat tussen de 8 en 63 tekens lang is. Dit wachtwoord kan zijn opgebouwd uit een combinatie van letters, cijfers en andere tekens. Elke cliënt maakt gebruik van dezelfde sleutel om toegang te krijgen tot het netwerk. Deze modus wordt doorgaans in een woonomgeving gebruikt.

WPA-Enterprise (RADIUS) is een configuratie waarin een radiusserver automatisch de sleutels aan de cliënten toekent. Van deze modus wordt doorgaans op kantoren gebruik gemaakt.

WPA-Personal (PSK) instellen

1. Selecteer "WPA/WPA2-PSK" in het dropdown-menu "Security Mode" (Beveiligingsmodus).
2. Selecteer "WPA-PSK" voor authentificatie.
3. Selecteer "TKIP" als "Encryption Technique" (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.
4. Voer uw "pre-shared key" in. Deze sleutel bestaat uit 8 tot 63 tekens, dit kunnen letters, cijfers of symbolen zijn. U dient bij al uw cliënten dezelfde sleutel te gebruiken. Uw PSK kan er als volgt uitzien: "Netwerksleutel familie Jansen".
5. Klik op "Apply Changes" (Wijzigingen aanbrengen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.

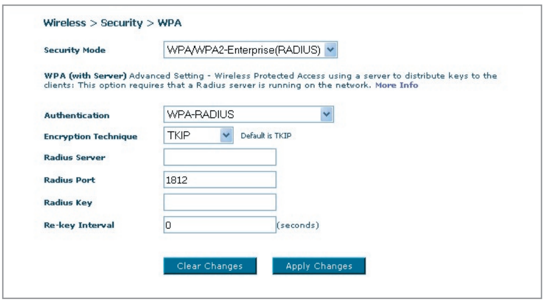


WPA-Enterprise (RADIUS) instellen

Als uw netwerk een radiusserver gebruikt om de sleutels aan de cliënten toe te wijzen, gebruik dan deze instelling.

1. Selecteer "WPA/WPA2—Enterprise (RADIUS)" in het dropdown-menu "Security Mode" (Beveiligingsmodus).

2. Selecteer "WPA-RADIUS" voor authentificatie
3. Selecteer "TKIP" als "Encryption Technique" (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.
4. Voer het IP-adres van de radiusserver in in de daarvoor bestemde velden.
5. Voer de radius-sleutel in in het veld "Radius Key".
6. Voer het sleutelinterval in. Het sleutelinterval geeft aan hoe vaak de sleutels worden verdeeld (in pakketten).
7. Klik op "Apply Changes" (Wijzigingen aanbrengen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.



Systeemvereisten voor WPA2

BELANGRIJK: Om WPA2-beveiliging te kunnen gebruiken moeten al uw computers en netwerkadapters geüpgradet zijn en beschikken over stuurprogramma's en software die WPA2 ondersteunen. U kunt gratis beveiligingspatches van Microsoft downloaden. Deze patches werkt alleen onder het Windows XP-besturingssysteem. Andere besturingssystemen worden op dit moment nog niet ondersteund.

Voor een computer met Windows XP zonder Service Pack 2 (SP2) kan via http://support.microsoft.com/?kbid=826942 gratis een bestand genaamd "Windows XP Support Patch for Wireless Protected Access (KB 826942)" gedownload worden van http://support.microsoft.com/?kbid=826942.

Voor Windows XP met Service Pack 2 heeft Microsoft een gratis download uitgebracht voor het bijwerken van uw draadloze cliëntcomponenten ter ondersteuning van WPA2 (KB893357). De update kunt u downloaden via: http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

1 2 3 4 5 6 7 8 9 10 Hoofdstuk

LET OP: U dient ook te controleren of al uw draadloze netwerkkaarten/ adapters WPA2 ondersteunen en dat u de nieuwste stuurprogramma's gedownload en geïnstalleerd hebt. Voor de meeste draadloze netwerkkaarten van Belkin is er een update voor stuurprogramma's beschikbaar op de website van Belkin: www.belkin.com/networking.

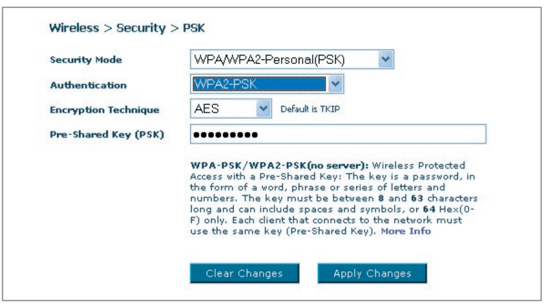
WPA2-Personal (PSK) instellen

1. Selecteer "WPA/WPA2-PSK (PSK)" in het dropdown-menu "Security Mode" (Beveligingsmodus).

2. Selecteer "WPA2-Personal (PSK)" voor authentificatie.

3. Selecteer "AES" als Encryption Technique (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.

4. Voer uw "pre-shared key" in. Deze sleutel bestaat uit 8 tot 63 tekens, dit kunnen letters, cijfers of symbolen zijn. U dient bij al uw cliënten dezelfde sleutel te gebruiken. Uw PSK kan er als volgt uitzien: "Netwerksleutel familie Jansen".



5. Klik op "Apply Changes" (Wijzigingen aanbrengen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.

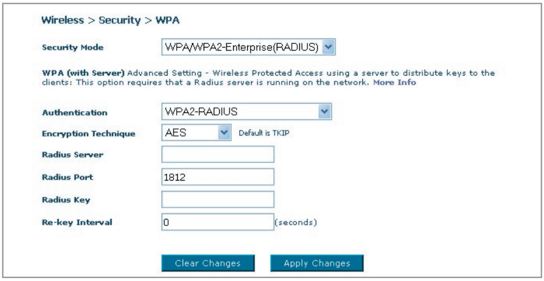
WPA2-Enterprise (RADIUS) instellen

Als uw netwerk een radiusserver gebruikt om de sleutels aan de cliënten toe te wijzen,

gebruik dan deze instelling.

1. Selecteer "WPA/WPA2—Enterprise (RADIUS)" in het dropdown-menu "Security Mode" (Beveligingsmodus).
2. Selecteer "WPA2-RADIUS" voor authentificatie.
3. Selecteer "AES" als Encryption Technique (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.

4. Voer het IP-adres van de radiusserver in in de daarvoor bestemde velden.
5. Voer de radius-sleutel in in het veld "Radius Key".
6. Voer het sleutelinterval in. Het sleutelinterval geeft aan hoe vaak de sleutels worden verdeeld (in pakketten).
7. Klik op "Apply Changes" (Wijzigingen aanbrengen) om te eindigen. Stel nu al uw cliënten op deze manier in.



BELANGRIJK: Zorg ervoor dat uw draadloze computers geüpdatet zijn, WPA2 ondersteunen en voorzien zijn van de juiste instellingen die een verbinding met de router mogelijk maken.

De beveiligingsinstellingen van de netwerkadapter van uw computer configureren

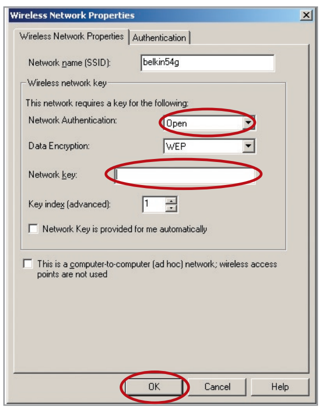
Opmerking: Deze paragraaf informeert u over hoe u uw netwerkadapter kunt configureren voor gebruik met beveiliging. Op dit moment zou u uw draadloze router of draadloos accesspoint al zo moeten hebben ingesteld dat deze gebruik maakt van WPA2, WPA of WEP. Om een draadloze verbinding tot stand te kunnen brengen dient u uw draadloze notebook- en desktopnetwerkkaart te configureren met dezelfde beveiligin gsinstellingen.

Belkin G+ MIMO netwerkkaarten worden geleverd met de praktische Wireless Networking Utility. Klik eenvoudigweg op uw de naam van uw draadloze netwerk (SSID) in het overzicht van beschikbare netwerken (Available Networks) en voer uw pre-shared key (PSK) in. Voor meer informatie verwijzen wij u naar de handleiding van de netwerkkaart van Belkin.

De meeste computers kunt u ook instellen voor het werken met een router via het Wireless Network Properties venster dat in uw Microsoft Windows besturingssysteem is ingebouwd ucan also setup to work with the Router from Wireless Network Properties screen build-in your Microsoft Windows operating system. Twee voorbeelden:

Uw computer aansluiten op een draadloos netwerk dat een 64-bits of 128-bits WEP-sleutel vereist.

1. Dubbelklik op het signaalindicatorpictogram om het venster “Wireless Network Utility” te laten verschijnen. Als u op de knop “Advanced” (Geavanceerd) drukt, kunt u meer opties van de draadloze netwerkkaart bekijken en configureren.
2. Op het tabblad “Wireless Network Properties” (Eigenschappen draadloos netwerk) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op “Configure” (Configureren).
3. Selecteer “WEP” onder “Data Encryption” (Dataencryptie)
4. Zorg ervoor dat de optie “The key is provided for me automatically” (De sleutel wordt automatisch verstrekt) niet is aangevinkt. Als u deze computer gebruikt om in te loggen op een bedrijfsnetwerk, vraag dan aan uw netwerkbeheerder of deze optie aangevinkt moet zijn of niet.
5. Typ de WEP-sleutel in in het daarvoor bestemde vakje bij “Network Key” (Netwerksleutel).

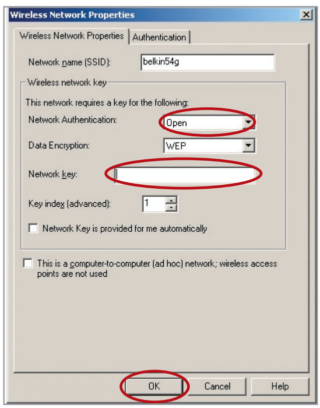


Belangrijk: Een WEP-sleutel is een combinatie van cijfers en letters van A tot F en 0 tot 9. Voor 128-bits WEP-encryptie dient u 26 hexadecimale tekens in te voeren. Voor 64-bits WEP-encryptie dient u 10 hexadecimale tekens in te voeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw draadloze router of accesspoint.

6. Klik op “OK” om de instellingen op te slaan.

Uw computer aansluiten op een draadloos netwerk dat WPA-PSK vereist (zonder server)

1. Dubbelklik op het signaalindicatorpictogram om het venster "Wireless Network Utility" te laten verschijnen. Als u op de knop "Advanced" (Geavanceerd) drukt, kunt u meer opties van de draadloze netwerkkaart bekijken en configureren.
2. Op het tabblad "Wireless Networks" (Draadloze netwerken) selecteert u een netwerknaam uit de lijst "Available networks" (Beschikbare netwerken) en vervolgens klikt u op "Configure" (Configureren).
3. Selecteer "WPA-PSK (no server)" onder "Network Authentication" (Netwerkauthentificatie).
4. Typ de WPA-sleutel in in het veld naast "Network Key" (Netwerksleutel).

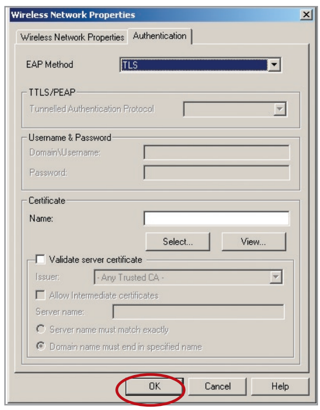


Belangrijk: WPA-PSK is opgebouwd uit een combinatie van cijfers en letters van A tot Z en 0 tot 9. Voor WPA-PSK kunt u 8 tot 63 tekens invoeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw draadloze router of accesspoint.

5. Klik op "OK" om de instellingen op te slaan.

Uw computer aansluiten op een draadloos netwerk dat WPA (met radiusserver) vereist

1. Dubbelklik op het signaalindicatorpictogram om het venster "Wireless Network Utility" te laten verschijnen. Als u op de knop "Advanced" (Geavanceerd) drukt, kunt u meer opties van de draadloze netwerkkaart bekijken en configureren.
2. Op het tabblad "Wireless Networks" (Draadloze netwerken) selecteert u een netwerknaam uit de lijst "Available networks" (Beschikbare netwerken) en vervolgens klikt u op "Configure" (Configureren).
3. Selecteer "WPA" onder "Network Authentication" (Netwerkauthentifi catie).
4. Selecteer op het tabblad "Authentication" (Authentificatie) de door uw netwerkbeheerder bepaalde vereiste instellingen.



5. Klik op "OK" om de instellingen op te slaan.

WPA/WPA2 instellen voor niet-Belkin draadloze desktop- en notebookkaarten

Voor niet-Belkin WPA draadloze desktop- en notebookkaarten die niet zijn voorzien van WPA/WPA2-software, kunt u gratis van de website van Microsoft een bestand downloaden met de naam "Windows XP Support Patch for Wireless Protected Access".

Let op: Dit Microsoft-bestand werkt alleen met Windows XP. Andere besturingssystemen worden op dit moment nog niet ondersteund.

Belangrijk: U dient ook te controleren of de kaartfabrikant WPA/WPA2 ondersteunt en of u het nieuwste stuurprogramma van hun support site hebt gedownload.

Ondersteunde besturingssystemen:
- **Windows XP Professional**
- **Windows XP Home Edition**

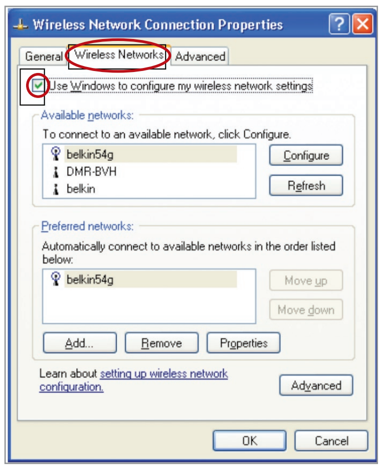
De Wireless Network Utility instellen voor Windows XP om gebruik te kunnen maken van WPA/WPA2-PSK

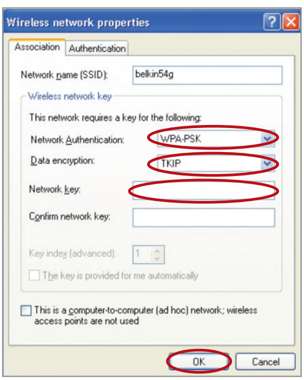
Om WPA-PSK te kunnen gebruiken, dient u ervoor te zorgen dat u Windows Wireless Network Utility gebruikt. Dit doet u als volgt:

1. In Windows XP, kjlikt u op “Start > Control Panel > Network Connections” (Start > Configuratiescherm > Netwerkverbindingen).

2. Klik met de rechter muisknop op “Wireless Network Connection” (Draadloze netwerkverbinding) en selecteer “Properties” (Eigenschappen).

3. Nadat u geklikt hebt op het tabblad “Wireless Networks” (Draadloze netwerken) verschijnt het volgende venster. Zorg ervoor dat het vakje “Use Windows to configure my wireless network settings” (Gebruik Windows om de instellingen van mijn draadloze netwerk te configureren) is aangevinkt.





4. Klik op het tabblad “Wireless Networks” (Draadloze netwerken) op de knop “Configure” (Configureren). Het volgende scherm zal verschijnen.

5. Voor een netwerk in uw woning of kantoor selecteert u onder “Network Authentication” (Netwerkauthentificatie) “WPA-PSK” of “WPA2-PSK”

Let op: Selecteer “WPA” als u deze computer gebruikt om verbinding te maken met een bedrijfsnetwerk dat een authentificatieserver ondersteunt, zoals bijvoorbeeld een radiusserver. Neem contact op met uw netwerkbeheerder voor nadere informatie.

6. Selecteer onder “Data Encryption” (Data-encryptie) “TKIP” of “AES”. Deze instelling moet gelijk zijn aan die van de router.

7. Typ de encryptiesleutel in in het vakje naast “Network Key” (Netwerksleutel).

Belangrijk: Voer uw Pre-Shared sleutel in. Deze sleutel bestaat uit 8 tot 63 tekens, dit kunnen letters, cijfers of symbolen zijn. U dient bij al uw cliënten dezelfde sleutel te gebruiken.

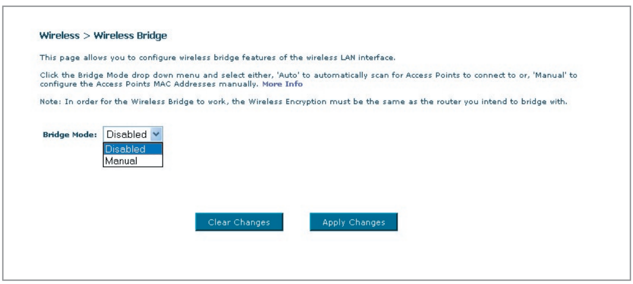
8. Klik op “OK” om de instellingen op te slaan.

Wireless Bridge (Draadloze brug)

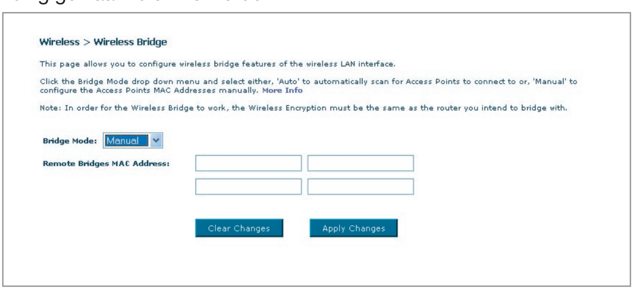
Wireless Bridging of Wireless Distribution System (WDS) wordt gebruikt om draadloze routers en accesspoints te verbinden ten behoeve van uitbreiding van een netwerk.

Klik op het dropdown-menu naast “Bridge Mode” en selecteer een van de volgende mogelijkheden:

Disabled (gedeactiveerd): Wireless Bridging deactiveren (standaard)



Handmatig: Handmatig de MAC-adressen invoeren van de accesspoints waarmee draadloos verbinding gemaakt dient te worden.



1 Draadloze kanalen dienen voor router en accesspoint gelijk te zijn.

2 Beveiligingsinstellingen (WEP) dienen voor router en accesspoint gelijk te zijn.

3 Indien MAC-filtering is gedeactiveerd, dient de gebruiker de WLAN Mac-adressen van de router en het accesspoint toe te voegen, zodat deze apparaten met elkaar kunnen communiceren.

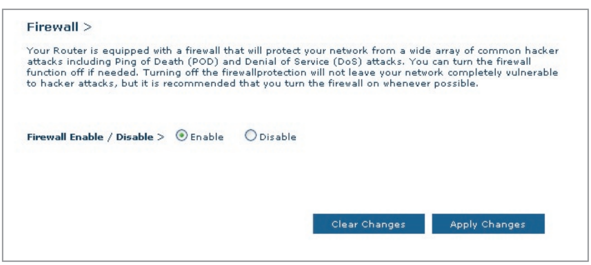
4 Indien uw netwerk is beveiligd via WPA-beveiliging dient de SSID voor beide accesspoints hetzelfde te zijn.

Firewall

Uw router is voorzien van een firewall die uw netwerk beschermt tegen uiteenlopende hackeraanvallen zoals:

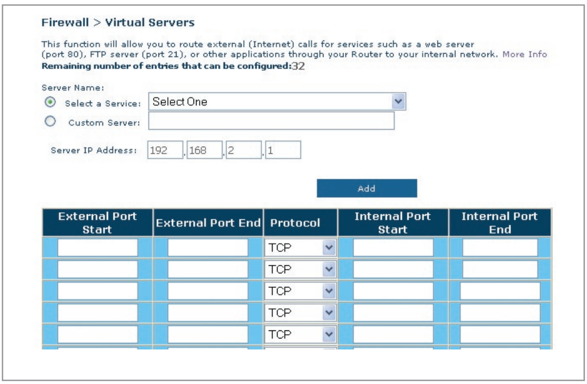
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP met lengte nul
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

De firewall schermt ook gewone poorten af die vaak gebruikt worden om netwerken aan te vallen. Deze poorten zijn dan onzichtbaar gemaakt waardoor zij voor hackers eenvoudigweg niet lijken te bestaan. U kunt de firewallfunctie eventueel uitschakelen hoewel het aanbeveling verdient de firewall ingeschakeld te laten. Het uitschakelen van de firewall laat uw netwerk niet volledig onbeschermd tegen een aanval van hackers, maar wij raden u toch aan de firewall geactiveerd te houden.



Virtuele servers

Via “Virtual Servers” kunt u externe (Internet)verbindingen voor diensten zoals een webserver (poort 80), FTP-server (poort 21), of andere applicaties, via uw router doorsturen naar uw interne netwerk. Aangezien uw interne computers beschermd worden door een firewall, kunnen computers buiten uw netwerk (via het Internet) de interne computers niet bereiken omdat ze niet “zichtbaar” zijn. Als u de functie “virtual server” voor een specifieke applicatie dient te configureren, neem dan contact op met de leverancier van de applicatie om geïnformeerd te worden over welke poortinstellingen u nodig hebt. U kunt deze poortgegevens handmatig invoeren in de router.



Een applicatie kiezen

U kunt kiezen uit een reeks populaire applicaties. Klik op “Select a Service” en selecteer de gewenste applicatie in het dropdown-menu. De instellingen worden overgebracht naar de eerste beschikbare regel. Klik op “Add” (Toevoegen) om de instelling voor deze applicatie op te slaan.

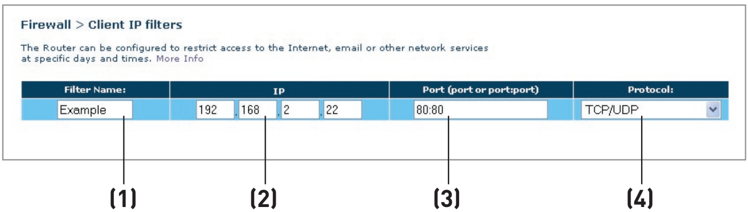
Instellingen handmatig in de virtuele server invoeren

Om handmatig instellingen te bepalen, klikt u op “Custom Server” en voert u een naam voor de server in. Voer het IP-adres van de server in in het vak voor de interne computer en geef aan welke poorten gepasseerd dienen te worden. Selecteer vervolgens het protocoltype (TCP of UDP) en klik op “Add” (Toevoegen).

U neemt een zeker risico door poorten in uw firewall te openen. U kunt instellingen zeer snel in- en uitschakelen. Wij adviseren deze instellingen uit te schakelen wanneer u een bepaalde toepassing niet gebruikt.

Cliënt IP-filters

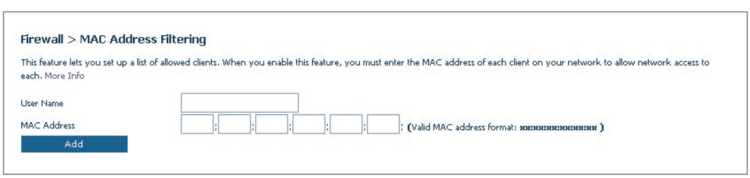
De router kan zo worden geconfigureerd dat toegang tot het Internet, e-mail, of andere netwerkdiensten op bepaalde dagen en tijden beperkt is.



Om bijvoorbeeld de toegang tot het Internet voor één enkele computer af te sluiten, voert u de naam van het filter in in het vakje voor “Filter Name” **(1)** voert u het IP-adres van de beoogde computer in het IP-veld in **(2)**. Vervolgens vult u in het poortveld “80:80” in **(3)**. Selecteer protocol in het dropdown-menu “Protocol” **(4)**. Klik op “Apply Changes” (Wijzigingen aanbrengen). De computer op het door u opgegeven IP-adres zal nu de toegang tot het Internet worden ontzegd.

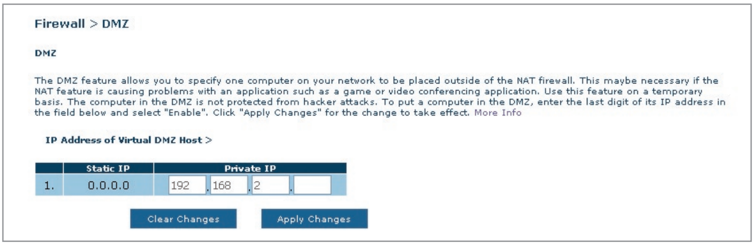
MAC-adressenfilter

Het MAC-adressenfilter is een krachtig beveiligingsinstrument waarmee u kunt aangeven welke computers toegang hebben tot het netwerk. Elke computer die probeert het netwerk binnen te komen maar die niet in de filterlijst voorkomt, wordt de toegang geweigerd. Wanneer u deze functie aanzet, moet u een naam voor de gebruiker en het MAC-adres invoeren van iedere cliënt (computer) op uw netwerk om elk van deze computers toegang te geven tot het netwerk. Klik op “Add” (Toevoegen) om de instellingen op te slaan.



DMZ (Gedemilitariseerde zone)

Indien een van uw cliënten van achter de firewall geen internetapplicatie kan draaien, kunt u deze cliënt onbeperkte tweewegs internettoegang verstrekken. Dit kan nodig zijn wanneer de NAT-functie problemen veroorzaakt met applicaties als games en videoconferenties. Schakel deze functie alleen tijdelijk in. **De computer in de gedemilitariseerde zone wordt namelijk NIET beschermd tegen hackeraanvallen.**

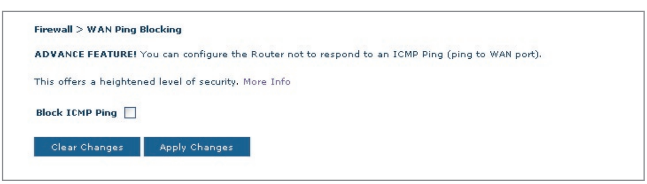


Om een computer in de gedemilitariseerde zone te plaatsen, dient u het LAN IP-adres van deze computer in het “Private IP”-veld in te vullen en te klikken op “Apply Changes” (Wijzigingen aanbrengen).

ICMP-pings blokkeren

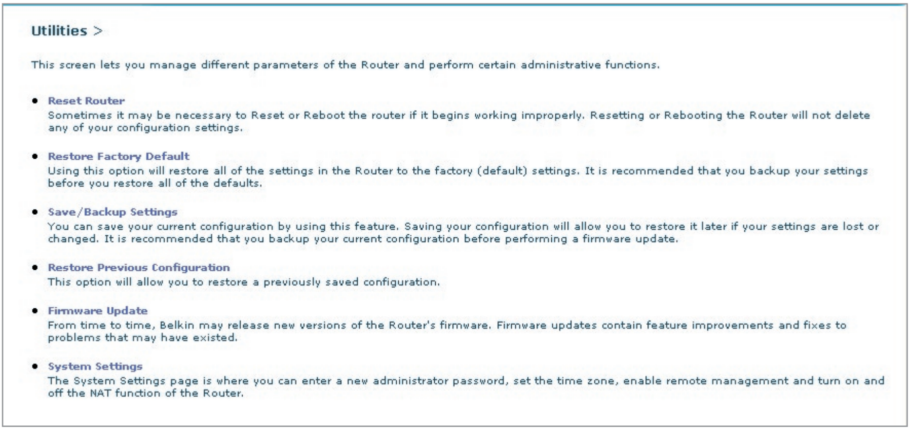
Computerhackers maken gebruik van een techniek die bekend is onder de naam “pingen” om potentiële slachtoffers op het Internet te vinden. Door naar een bepaald IP-adres te pingen en een reactie te ontvangen van het IP-adres, kan een hacker vaststellen of zich daar misschien iets interessants bevindt. De router kan zo worden ingesteld dat hij niet op ICMP-pings van buiten reageert. Hierdoor wordt de veiligheidsmarge van uw router verhoogd.

Om het ping-antwoordbericht uit te schakelen, selecteert u “Block ICMP Ping” (ICMP-ping blokkeren) **(1)** en klikt u op “Apply Changes” (Wijzigingen aanbrengen). De router reageert nu niet op een ICMP-ping.



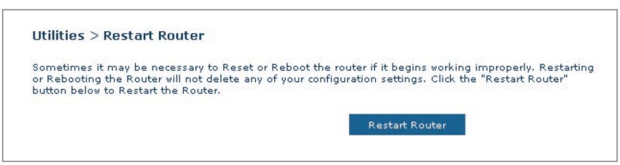
Utilities (Hulpprogramma's)

In het scherm "Utilities" (Hulpprogramma's), kunt u verschillende parameters van de router beheren en bepaalde beheerfuncties uitvoeren.



De router herstarten

Als de werking van de router niet meer optimaal is, kan het soms nodig zijn de router opnieuw te starten. De configuratie-instellingen van de router worden door opnieuw starten NIET gewist.



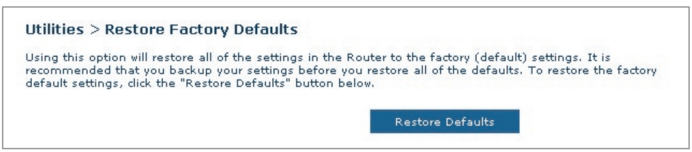
De router opnieuw starten om de normale werking te herstellen

1. Klik op de knop "Restart Router" (Router opnieuw opstarten).
2. De volgende melding verschijnt. Klik op "OK" om uw router te herstarten.

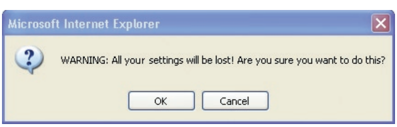


De standaard fabrieksinstellingen herstellen

Wanneer u deze optie gebruikt, worden alle instellingen in de router naar de (standaard-) fabrieksinstellingen teruggezet. Het is verstandig eerst van uw eigen instellingen een reservekopie te maken voordat u de standaardinstellingen herstelt.

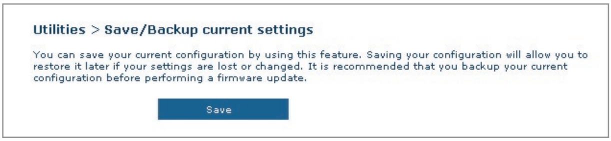


1. Klik op de knop "Restore Defaults" (Standaard instellingen herstellen).
2. De volgende melding verschijnt. Klik op "OK" om de standaard fabrieksinstellingen te herstellen.

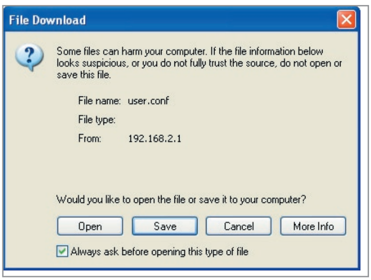


Huidige instellingen opslaan/als backupbestand opslaan

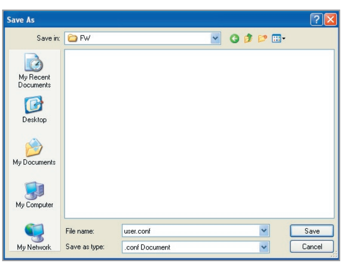
Met behulp van deze functie kunt u de huidige configuratie opslaan. Door een reservekopie te maken van uw huidige configuratie kunt u deze later in het geval van verlies of wijziging herstellen. Het is raadzaam een reservekopie te maken van uw huidige configuratie voordat u uw firmware bijwerkt.



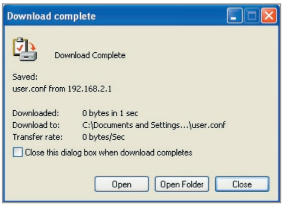
1. Klik op "Save" (Opslaan). Er gaat een venster open met de naam "File Download" (Bestand downloaden). Klik op "Save" (Opslaan).



2. Een scherm wordt geopend waarin u de locatie kunt selecteren waar u het configuratiebestand wilt opslaan. Selecteer een locatie. U kunt zelf bepalen hoe u het bestand noemt. Wij raden u echter aan er bij de naamgeving rekening mee te houden dat u het besatnd nog wel terug moet kunnen vinden. Wanneer u de locatie hebt geselecteerd en de naam van het bestand hebt ingevoerd, klikt u op "Save" (Opslaan).



3. Als het bestand is opgeslagen, verschijnt het volgende scherm. Klik op “Close” (Sluiten).

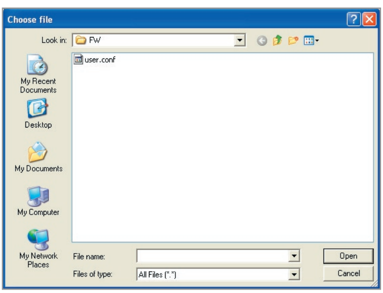


De configuratie is nu bewaard.

Vorige instellingen herstellen

Met deze optie kunt u een eerder opgeslagen configuratie herstellen.

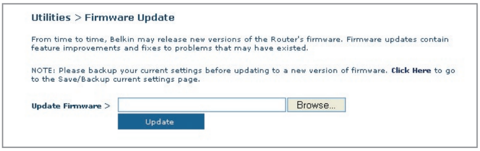
1. Klik op “Browse” (Bladeren). Er gaat een venster open waarin u de locatie van het configuratiebestand kunt selecteren. Alle configuratiebestanden hebben de extensie “.conf”. Zoek het configuratiebestand op dat u wilt herstellen en dubbelklik erop.



2. Klik op “Open” (Openen).

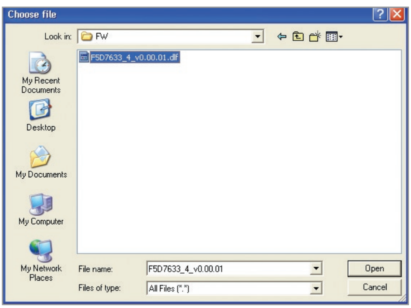
Firmware bijwerken

Af en toe brengt Belkin een nieuwe versie uit van de firmware voor de router. Nieuwe firmwareversies bevatten verbeteringen van functies en oplossingen voor eventuele problemen. Wanneer Belkin nieuwe firmware uitbrengt, kunt u deze downloaden van de website en de firmware van de router bijwerken tot en met de nieuwste versie.



De firmware van de router bijwerken

1. Op de pagina “Firmware Update” (Firmware bijwerken) klikt u op “Browse” (Bladeren). Er gaat een venster open waarin u de locatie van het bijgewerkte firmwarebestand kunt selecteren.



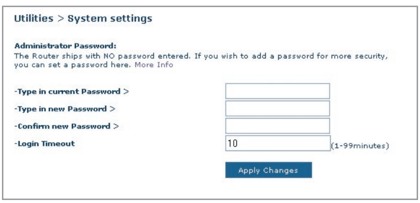
2. Ga naar het firmwarebestand dat u hebt gedownload. Selecteer het bestand door dubbel te klikken op de bestandsnaam.
3. Klik op “Update” (Bijwerken) om te upgraden naar de nieuwste firmwareversie.

Systeeminstellingen

Op de pagina “System Settings” (Systeeminstellingen) kunt u een nieuw wachtwoord invoeren voor de systeembeheerder, de tijdzone instellen, beheer op afstand inschakelen, en de UPnP-functie van de router aan- en uitschakelen.

Het wachtwoord voor de systeembeheerder instellen of wijzigen

De router wordt geleverd ZONDER vooraf geprogrammeerd wachtwoord. Als u een wachtwoord wilt toevoegen voor meer beveiliging, dan kunt u hier een wachtwoord instellen. Schrijf het wachtwoord op en bewaar het op een veilige plaats, aangezien u het nodig heeft als u in de toekomst wilt inloggen op de router. Het is ook verstandig een wachtwoord in te stellen als u van plan bent de mogelijkheid van extern beheer van uw router te gebruiken.



De inlog-timeout wijzigen

Met de optie inlog-timeout kunt u de maximale tijdsduur instellen waarbinnen u ingelogd kunt blijven op de Advanced Setup Interface (Geavanceerde setup-interface) van de router. De tijdklok begint te lopen als er geen activiteit is geweest. U hebt bijvoorbeeld een aantal wijzigingen in de geavanceerde gebruikersinterface aangebracht en daarna uw computer alleen gelaten zonder op “Logout” (Afmelden) te klikken. Als de timeout is ingesteld op 10 minuten, dan loopt de inlogsessie 10 minuten nadat u de router alleen hebt gelaten af. Als u meer wijzigingen wilt aanbrengen, dient u opnieuw op de router in te loggen. Deze inlog-timeoutoptie is bedoeld als extra beveiliging en staat standaard ingesteld op 10 minuten.

Opmerking: Er kan slechts één computer tegelijk ingelogd zijn op de Advanced Setup-interface van de router.

Tijd en tijdzone instellen

De tijdklok van de router wordt geregeld via de aansluiting op een SNTP (Simple Network Time Protocol) server. Hierdoor loopt de systeemklok van de router synchroon met de tijd van het wereldwijde internet. De gesynchroniseerde klok in de router wordt gebruikt voor de registratie van de beveiligingslog en de aansturing van het cliëntenfilter.

Selecteer de gewenste NTP-tijdservers en de tijdzonde waarin u zich bevindt, en klik vervolgens op “Apply Changes” (Wijzigingen aanbrengen). De systeemklok geeft niet onmiddellijk na inschakeling de juiste tijd aan. De router heeft ten minste 15 minuten nodig om een verbinding op te bouwen met de tijdservers op het Internet en voor het ontvangen van een antwoordsignaal. U kunt de klok niet zelf instellen.



Beheer op afstand activeren

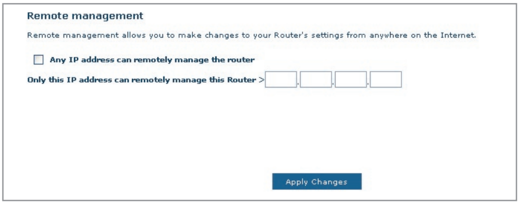
Voordat u deze geavanceerde functie van uw router van Belkin inschakelt, **DIENT U ERVOOR TE ZORGEN DAT U HET WACHTWOORD VOOR DE SYSTEEMBEHEERDER HEBT INGESTELD**. De functie “Remote Management” (Beheer op afstand) biedt u de mogelijkheid vanaf elke internetlocatie ter wereld de instellingen van uw router te wijzigen.

Klik op de knop “Change Settings” (Instellingen wijzigen) om de pagina voor “Remote Management” (Beheer op afstand) te openen.

Er zijn twee methoden voor het op afstand beheren van de router. Met de eerste kunt u de router vanaf elke internetlocatie openen door het selecteren van “Any IP address can remotely manage the Router” (Elk IP-adres kan de router op afstand beheren). Wanneer u uw WAN IP-adres intypt vanaf iedere willekeurige computer op het Internet, dan krijgt u een inlogscherm te zien waarin u het wachtwoord van uw router moet invoeren.

De tweede methode is een specifiek IP-adres uitsluitend te bestemmen voor beheer op afstand. Deze methode is veiliger, maar minder praktisch. Bij deze methode vult u in de daarvoor bestemde ruimte het IP-adres in van de computer waarmee u toegang tot de router wilt hebben en selecteert u “Only this IP address can remotely manage the Router” (Uitsluitend dit IP-adres kan de router op afstand beheren). Voordat u deze functie inschakelt, RADEN WIJ U TEN ZEERSTE AAN uw systeembeheerderwachtwoord in te stellen. Als u geen wachtwoord invult, loopt uw router het risico van indringers.

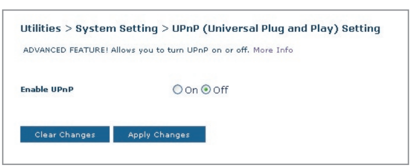
Klik op de knop “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan.



UPnP inschakelen/uitschakelen

UPnP (Universal Plug-and-Play) is weer een andere geavanceerde mogelijkheid van uw router van Belkin. Het is een technologie die naadloze voice- en video-messaging, games en andere applicaties mogelijk maakt die voldoen aan UPnP. Voor sommige applicaties dient de firewall van de router op een specifieke manier geconfigureerd te zijn voor een juiste werking. Hiervoor moeten doorgaans de TCP- en UDP-poorten worden geopend en in sommige gevallen triggerpoorten worden ingesteld. Applicaties die voldoen aan UpnP kunnen met de router communiceren, in principe om de router te “vertellen” op welke wijze de firewall moet worden geconfigureerd. Bij aflevering is de UPnP-functie van de router uitgeschakeld. Als u applicaties gebruikt die voldoen aan UpnP en u wilt profiteren van de mogelijkheden van UPpnP dan heeft het zin de UPnP-functie te activeren.

Klik op de knop “Change Settings” (Instellingen wijzigen) om de pagina voor “UPnP Setting” (UPnP-instelling) te openen. Selecteer vervolgens “On” (Aan) naast “Enable UPnP” (UPnP activeren) om UPnP te activeren. Klik op de knop “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan.



Probleem:

De ADSL-LED brandt niet.

Oplossing:

1. Controleer de verbinding tussen de router en de ADSL-lijn. Zorg ervoor dat de kabel van de ADSL-lijn is aangesloten op de poort van de router die wordt aangeduid met “DSL line”.
2. Zorg ervoor dat de router van stroom wordt voorzien. De LED voor Voeding op het frontpaneel zou nu moeten branden.

Probleem:

De Internet-LED brandt niet.

Oplossing:

1. Zorg ervoor dat de kabel van de ADSL-lijn is aangesloten op de poort van de router die wordt aangeduid met “DSL line” en dat de ADSL-LED brandt.
2. Zorg ervoor dat u over de juiste, door uw Internet Service Provider verstrekte, gegevens voor VPI/VCI, gebruikersnaam en wachtwoord beschikt.

Probleem:

Mijn type verbinding is “Static IP Address” (Statisch IP-adres). Ik kan geen verbinding met het Internet tot stand brengen

Oplossing:

Omdat uw type verbinding dat van een statisch IP-adres is, moet uw internet-serviceprovider u een IP-adres, een subnetmasker en een gateway-adres toewijzen. In plaats van gebruik te maken van de Wizard, gaat u naar “Connection Type” (Verbindingstype) en selecteert u het type verbinding. Klik op “Next” (Volgende) en selecteer “Static IP” (Statisch IP). Vervolgens voert u het IP-adres, subnetmasker en de standaard gateway-informatie in.

Probleem:

Ik ben mijn wachtwoord kwijt of vergeten.

Oplossing:

Druk de “Reset”-knop op het achterpaneel gedurende 10 seconden in om de standaard fabrieksinstellingen te herstellen.

Probleem:

Mijn draadloze PC kan geen verbinding maken met de router.

Oplossing:

1. Zorg ervoor dat de draadloze PC dezelfde SSID-instellingen heeft als de router en dat de beveiligingsinstellingen voor de cliënten, zoals WPA-beveiliging of WEP-encryptie, hetzelfde zijn.
2. Zorg ervoor dat de afstand tussen de router en de draadloze PC niet te groot is.

Probleem:

Het draadloze netwerkverbinding wordt vaak onderbroken.

Oplossing:

1. Zet uw draadloze PC dichter bij de router voor een beter signaal.
2. Er kan ook sprake zijn van interferentie, mogelijk veroorzaakt door de aanwezigheid van een magnetron of 2,4GHz draadloze telefoon. Wijzig de locatie van de router of maak gebruik van een ander draadloos kanaal.

Probleem:

Ik kan geen draadloze verbinding met het Internet tot stand brengen.

Oplossing:

Indien u vanaf een draadloze computer geen verbinding met het Internet tot stand kunt brengen, ga dan als volgt te werk:

1. Kijk naar de lampjes op uw router. Indien u gebruik maakt van een router van Belkin geldt het volgende voor de lampjes:
   - De LED voor Voeding zou moeten branden.
   - De DSL-LED zou niet moeten knipperen en continu moeten branden.
   - De “Internet LED” zou continu moetenbranden of moeten knipperen.
2. Open de wireless utility software door te klikken op het pictogram rechts onderin het scherm. Indien u een draadloze kaart van Belkin gebruikt, zou het pictogram in de taakbalk er als volgt uit moeten zien:  Het pictogram kan rood of groen zijn.
3. Het precieze venster dat geopend wordt, is afhankelijk van het type draadloze kaart waarvan u gebruik maakt; onderdeel van alle utilities is echter een overzicht van “Available Networks” (Beschikbare netwerken)—de draadloze netwerken waarmee verbinding gemaakt kan worden.

Komt de naam van uw draadloze netwerk in dit overzicht voor?

Ja, de naam van mijn netwerk wordt vermeld.—Ga naar de paragraaf “Ik kan geen draadloze verbinding met het Internet tot stand brengen maar de naam van mijn netwerk is bekend” onder Problemen oplossen.

Nee, de naam van mijn netwerk wordt niet genoemd.—Ga naar de paragraaf “Ik kan geen draadloze verbinding met het Internet tot stand brengen en de naam van mijn netwerk is niet bekend”.

Probleem:

Ik kan geen draadloze verbinding met internet tot stand brengen, maar de naam van mijn netwerk is bekend.

Oplossing:

Indien de juiste netwerknaam is opgenomen in het overzicht van “Available Networks” (Beschikbare netwerken), volg dan de onderstaande stappen om een draadloze verbinding tot stand te brengen.

1. Klik op de juiste netwerknaam in het overzicht met beschikbare netwerken.
2. Indien voor het netwerk beveiligingsinstellingen (encryptie) zijn geactiveerd, dient u de netwerksleutel in te voeren. Meer informatie over beveiliging vindt u in het hoofdstuk Beveiligingsinstellingen van uw draadloze netwerk wijzigen
3. Binnen enkele seconden wordt het pictogram in de taakbalk, links onderin uw scherm, groen. Zo wordt aangegeven dat er een verbinding met het netwerk tot stand is gebracht.



Probleem:

Ik kan geen draadloze verbinding met het Internet tot stand brengen en de naam van mijn netwerk is niet bekend.

Oplossing

Doorloop onderstaande stappen als de naam van uw netwerk niet is opgenomen in het overzicht “Available Networks” (Beschikbare netwerken) in het hulpprogramma:

1. Verplaats, indien mogelijk, de computer tijdelijk op een afstand van tussen anderhalve en drie meter van de router vandaan. Sluit

de utility en heropen hem. Als de naam van het netwerk nu wel in het overzicht “Available Networks” (beschikbare netwerken) verschijnt, hebt u mogelijk een probleem met het bereik of last van storing. Wij verwijzen u ook naar Appendix B, getiteld “Belangrijke factoren die een rol spelen bij plaatsing en setup”.

2. Gebruik een computer die via een netwerkkabel op de router is aangesloten (in plaats van een draadloze verbinding) en zorg dat “Broadcast SSID” is ingeschakeld. Deze instelling vindt u op de pagina voor het configureren van “Channel and SSID” (Kanaal en SSID).

   Als u nog steeds geen toegang tot Internet kunt krijgen nadat u deze stappen heeft doorlopen, neem dan contact op met de afdeling Technische Ondersteuning van Belkin.

Probleem:

De prestaties van mijn draadloze netwerk zijn wisselvallig.
De gegevensoverdracht geschiedt soms traag.
Het signaal is zwak.
Problemen bij het tot stand brengen/behouden van een Virtual Private Network-verbinding.

Oplossing:

Draadloze technologie is gebaseerd op radiogolven. Dit betekent dat de connectiviteit en de doorvoersnelheid afnemen naarmate de afstand tussen de apparaten groter is. Andere factoren die een vermindering van de signaalkwaliteit veroorzaken (metaal is meestal de grootste boosdoener) zijn muren en metalen apparaten. Hierdoor is het bereik van draadloze apparatuur binnenshuis meestal zo’n 30 tot 60 meter. Hou er verder rekening mee dat de snelheid van de verbinding af zal nemen naarmate de afstand tot de router of het accesspoint groter wordt.

Om vast te stellen of problemen met draadloze gegevensoverdracht te maken hebben met afstand, adviseren we u uw computer tijdelijk te verplaatsen, indien mogelijk, op een afstand van 1,5 tot 3 meter van de router.

Het draadloze kanaal wijzigen - Het wijzigen van het kanaal kan een positief effect hebben op de prestaties en betrouwbaarheid van uw draadloze netwerk indien ander draadloos verkeer in uw omgeving en interferentie de prestaties van uw netwerk negatief beïnvloeden. Het standaard ingestelde kanaal van de router is 11. Afhankelijk van uw regio kunt u voor verschillende andere kanalen kiezen. Raadpleeg op pagina 37 de paragraaf “Het kanaal voor draadloze communicatie wijzigen” voor meer informatie over het kiezen van een kanaal.

De overdrachtssnelheid verlagen - Het verlagen van de overdrachtssnelheid kan het draadloze bereik en de stabiliteit van de verbinding verhogen. Bij de meeste draadloze netwerkkaarten kan de overdrachtssnelheid aangepast worden. Als u deze eigenschap wilt wijzigen, gaat u naar het “Controle Panel” (Configuratiescherm) in Windows, opent u de map “Network connections” (Netwerkverbindingen) en dubbelklikt u op de verbinding van uw draadloze kaart. Onder “Properties” (Eigenschappen) selecteert u de knop “Configure” (Configureren) op het tabblad “General” (Algemeen). (Gebruikers van Windows 98 dienen de draadloze kaart te selecteren en op “Properties” (Eigenschappen) te klikken.) Vervolgens selecteert u op het tabblad “Advanced” (Geavanceerd) de overdrachtssnelheid. Draadloze cliëntkaarten regelen doorgaans automatisch de draadloze overdrachtssnelheid voor u, maar dit kan periodiek onderbreking van de verbinding veroorzaken als het draadloze signaal te zwak is; in de regel zijn langzamere overdrachtssnelheden betrouwbaarder. Experimenteer met verschillende verbindingssnelheden totdat u de beste verbinding voor uw netwerkomgeving gevonden hebt; de beschikbare overdrachtssnelheden zouden allemaal geschikt moeten zijn voor internetgebruik. Raadpleeg voor meer informatie de handleiding bij uw netwerkkaart.

Probleem:

Ik heb problemen met het installeren van Wired Equivalent Privacy of WEP-beveiliging op een router of accesspoint van Belkin

Oplossing

1. Log in op uw draadloze router of accesspoint.
2. Open uw webbrowser en typ het IP-adres van uw router accesspoint in. (De standaardinstelling voor de router is 192.168.2.1, die voor het 802.11g accesspoint is 192.168.2.254). Log in op uw router door op de knop “Login” in de rechter bovenhoek van uw scherm te drukken. U wordt gevraagd uw wachtwoord in te voeren. Als u geen wachtwoord hebt ingesteld dan vult u dit veld niet in en klikt u op “Submit” (indienen).
3. Klik op het tabblad “Wireless” (Draadloos) links op uw scherm. Selecteer het “Encryption” (Encryptie) of “Security” (Beveiliging) tabblad om naar de instellingenpagina voor beveiliging te gaan.
4. Selecteer “128-bit WEP” in het dropdown-menu.
5. Nadat u een WEP-encryptiemodus heeft geselecteerd, kunt u uw hexadecimale WEP-sleutel handmatig intypen of een passphrase in het “Passphrase”-veld invoeren en klikken op “Generate” (Genereren) om uit de passphrase een WEP-sleutel te genereren. Klik op “Apply

Changes" (Wijzigingen toepassen) om te eindigen. Zorg er nu voor dat al uw cliënten op deze manier zijn ingesteld. Een hexadecimale sleutel is een combinatie van cijfers en letters van A tot F en 0 tot 9. Voor 128-bits WEP dient u 26 hexadecimale tekens in te voeren.
Bijvoorbeeld:
C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bits sleutel

6. Klik op "Apply Changes" (Wijzigingen aanbrengen) om te eindigen. De encryptie in de router is nu ingesteld. Iedere computer binnen uw draadloze netwerk moet nu worden geconfigureerd met dezelfde beveilig ingsinstellingen.

WAARSCHUWING: Als u de draadloze router of accesspoint vanaf een computer met een draadloze cliënt configureert, dient u ervoor te zorgen dat de beveiliging voor die draadloze cliënt is ingeschakeld. Als dat niet gebeurt, krijgt u geen draadloze verbinding.

Opmerking voor Mac-gebruikers: De oorspronkelijke Apple AirPort®-producten ondersteunen uitsluitend
64-bits encryptie. Apple AirPort 2-producten kunnen 64-bits en 128-bits encryptie ondersteunen. Controleer dus eerst het type Apple Airport-product dat u gebruikt. Als het u niet lukt uw netwerk met 128-bits encryptie te configureren, probeer dan 64-bits encryptie.

Probleem:

Ik heb problemen met het installeren van Wired Equivalent Privacy of WEP-beveiliging op een draadloze netwerkkaart van Belkin

Oplossing:

De draadloze netwerkkaart dient dezelfde sleutel te gebruiken als de draadloze router of het draadloze accesspoint. Als uw draadloze router of accesspoint de sleutel 00112233445566778899AABBCC gebruikt, dan moet voor de draadloze kaart exact dezelfde sleutel worden ingesteld.

1. Dubbelklik op het signaalindicatorpictogram om het venster "Wireless Network" (Draadloos netwerk) te laten verschijnen.
2. Met de knop "Advanced" (Geavanceerd) kunt u meer opties van de kaart bekijken en configureren.
3. Nadat u op "Advanced" (Geavanceerd) hebt geklikt, verschijnt de Belkin Wireless LAN Utility. Met dit hulpprogramma kunt u alle geavanceerde functies van de draadloze kaart van Belkin beheren.
4. Op het tabblad "Wireless Networks Properties" (Eigenschappen draadloze netwerken) selecteert u een netwerknaam uit de lijst "Available networks" (Beschikbare netwerken) en vervolgens klikt u op de knop "Properties"

(Eigenschappen).

5. Selecteer “WEP” onder “Data Encryption” (Dataencryptie)
6. Zorg ervoor dat het selectievakje “The key is provided for me automatically” (Ik krijg de sleutel automatisch), onderaan, niet is aangevinkt. Als u deze computer gebruikt om in te loggen op een bedrijfsnetwerk, vraag dan aan uw netwerkbeheerder of deze optie aangevinkt moet zijn of niet.
7. Typ de WEP-sleutel in in het daarvoor bestemde vakje bij “Network Key” (Netwerksleutel).

   Belangrijk: Een WEP-sleutel is een combinatie van cijfers en letters van A tot F en 0 tot 9. Voor 128-bits WEP-encryptie dient u 26 hexadecimale sleutels in te voeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw draadloze router of accesspoint.

   Bijvoorbeeld: **C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4** = 128-bits sleutel
8. Klik op “OK” en vervolgens op “Apply” (Toepassen) om de instellingen op te slaan.

Indien u **GEEN** draadloze netwerkkaart van Belkin gebruikt, raden wij u aan de handleiding van u van de fabrikant van dat product hebt gekregen, te raadplegen.

Probleem:

Ondersteunen de producten van Belkin WPA?

Oplossing

Let op: Om WPA-beveiliging te kunnen gebruiken moeten al uw cliënten geüpgraded zijn naar stuurprogramma’s en software die WPA ondersteunen. U kunt gratis een beveiligingspatch van Microsoft downloaden. Deze patch werkt alleen onder het Windows XP-besturingssysteem.

U kunt deze patch hier downloaden:
http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

U dient tevens van de website van Belkin het nieuwste stuurprogramma te downloaden voor uw draadloze 802.11g desktop- of notebooknetwerkkaart van Belkin. Andere besturingssystemen worden op dit moment nog niet ondersteund. De patch van Microsoft ondersteunt uitsluitend apparaten zoals 802.11g-producten van Belkin met stuurprogramma’s die WPA ondersteunen.

De nieuwste stuurprogramma’s kunt u hier downloaden: http://web.belkin.com/support/networkingsupport.asp.

WPA-ondersteuning zal automatisch worden geïnstalleerd als u een upgrade van uw systeem doet naar Windows XP Service pack 2. Voor meer informatie kunt u terecht op: http://support.microsoft.com

Probleem:

Ik heb problemen bij het instellen van Wi-Fi Protected Access (WPA) beveiliging voor mijn draadloze router of accesspoint van Belkin in een thuisnetwerk.

Oplossing:

1. Selecteer "WPA-PSK (zonder server)" in het dropdown-menu "Security Mode" (Beveiligingsmodus).
2. Selecteer "TKIP" of "AES" als Encryption Technique (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.
3. Voer uw "pre-shared key" in. Deze kan bestaan uit 8 tot 63 karakters en wordt opgebouwd uit letters, cijfers, symbolen en spaties. U dient bij al uw cliënten dezelfde sleutel te gebruiken. Uw PSK kan er als volgt uitzien: "Netwerksleutel familie Jansen".
4. Klik op "Apply Changes" (Wijzigingen aanbrengen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.

Probleem:

Ik heb problemen met het installeren van Wi-Fi Protected Access (WPA) beveiliging op een router / accesspoint van Belkin voor een zakelijk netwerk.

Oplossing:

Als uw netwerk een radiusserver gebruikt om de sleutels aan de cliënten toe te wijzen, gebruik dan deze instelling. Van deze modus wordt doorgaans op kantoren gebruik gemaakt.

1. Selecteer "WPA (met server)" in het dropdown-menu "Security Mode" (Beveiligingsmodus).
2. Selecteer "TKIP" of "AES" als Encryption Technique (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.
3. Voer het IP-adres van de radiusserver in in de daarvoor bestemde velden.
4. Voer de radius-sleutel in in het veld "Radius Key".
5. Voer het sleutelinterval in. Het sleutelinterval geeft aan hoe vaak de sleutels worden verdeeld (in pakketten).
6. Klik op "Apply Changes" (Wijzigingen aanbrengen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.

Probleem:

Ik heb problemen met het installeren van Wi-Fi Protected Access (WPA) beveiliging op een draadloze netwerkkaart van Belkin voor een thuisnetwerk.

Oplossing:

Cliënten moeten dezelfde sleutel gebruiken als de draadloze router / accesspoint. Als bijvoorbeeld de sleutel “Netwerksleutel familie Jansen” door de draadloze router of het draadloze accesspoint wordt gebruikt, moeten de ook cliënten van diezelfde sleutel gebruik maken.

1. Dubbelklik op het signaalindicatorpictogram om het scherm “Wireless Network” te laten verschijnen.
2. Als u op de knop “Advanced” (Geavanceerd) drukt, kunt u meer opties van de kaart bekijken en configureren.
3. Nadat u op “Advanced” (Geavanceerd) hebt geklikt, verschijnt de Belkin Wireless LAN Utility. Met dit hulpprogramma kunt u alle geavanceerde functies van de draadloze kaart van Belkin beheren.
4. Op het tabblad “Wireless Networks Properties” (Eigenschappen draadloze netwerken) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op de knop “Properties” (Eigenschappen).
5. Selecteer “WPA-PSK (no server)” (WPA-PSK (zonder server)) onder “Network Authentication” (Netwerkauthentificatie).
6. Typ de WPA-sleutel in in het daarvoor bestemde vakje bij “Network Key” (Netwerksleutel)

Belangrijk: WPA-PSK is opgebouwd uit een combinatie van cijfers en letters van A tot Z en 0 tot 9. Voor WPA-PSK kunt u 8 tot 63 tekens invoeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw draadloze router of accesspoint.

7. Klik op “OK” en vervolgens op “Apply” (Toepassen) om de instellingen op te slaan.

Probleem:

Ik heb problemen met het installeren van Wi-Fi Protected Access (WPA) beveiliging op een draadloze netwerkkaart van Belkin voor een kantoornetwerk.

Oplossing:

1. Dubbelklik op het signaalindicatorpictogram om het scherm “Wireless Network” te laten verschijnen.
2. Als u op de knop “Advanced” (Geavanceerd) drukt, kunt u meer opties van de kaart bekijken en configureren.
3. Nadat u op “Advanced” (Geavanceerd) hebt geklikt, verschijnt de Belkin

Wireless LAN Utility. Met dit hulpprogramma kunt u alle geavanceerde functies van de draadloze kaart van Belkin beheren.

4. Op het tabblad “Wireless Networks Properties” (Eigenschappen draadloze netwerken) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op de knop “Properties” (Eigenschappen).
5. Selecteer “WPA” onder “Network Authentication” (Netwerkauthentificatie)
6. Selecteer op het tabblad “Authentication” (Authentificatie) de door uw netwerkbeheerder bepaalde vereiste instellingen.
7. Klik op “OK” en vervolgens op “Apply” (Toepassen) om de instellingen op te slaan.

Probleem:

Ik heb problemen met het installen van Wi-Fi Protected Access (WPA) beveiliging en ik maak **GEEN** gebruik van een draadloze netwerkkaart van Belkin voor een thuisnetwerk.

Oplossing:

Als u **GEEN** gebruik maakt van een draadloze desktop- en notebookkaart van Belkin en uw kaart niet voorzien is van software die WPA ondersteunt, dan kunt u gratis van de website van Microsoft een bestand downloaden met de naam “Windows XP Support Patch for Wireless Protected Access”. De patch van Microsoft kunt u downloaden door de knowledge base voor Windows XP WPA te doorzoeken.

Opmerking: Dit Microsoft-bestand werkt alleen met Windows XP. Andere besturingssystemen worden op dit moment nog niet ondersteund. U dient ook te controleren of de kaartfabrikant WPA ondersteunt en of u het nieuwste stuurprogramma van hun support site hebt gedownload.

Ondersteunde besturingssystemen:

- Windows XP Professional
- Windows XP Home Edition

Inschakelen WPA-PSK (zonder server)

1. In Windows XP klikt u op “Start > Control Panel > Network Connections” (Start > Configuratiescherm > Netwerkverbindingen).
2. Klik met de rechtermuisknop op het tabblad “Wireless Networks” (Draadloze netwerken). Het volgende scherm verschijnt. Zorg ervoor dat de optie “Use Windows to configure my wireless network settings” (Gebruik Windows om de instellingen van mijn draadloze netwerk te configureren) is aangevinkt.
3. Klik op het tabblad “Wireless Networks” (Draadloze netwerken) op

de knop “Configure” (Configureren). Het volgende venster zal verschijnen.

4. Voor gebruik in uw woning of op een klein kantoor, selecteert u onder “Network Administration” (Netwerkbeheer) “WPA-PSK”.

Opmerking: Selecteer “WPA (with radius server)” (WPA met radiusserver) als u deze computer gebruikt om verbinding te maken met een bedrijfsnetwerk dat een authenticatieserver ondersteunt, bijv. een radiusserver. Neem voor meer informatie contact op met uw netwerkbeheerder.

5. Selecteer onder “Data Encryption” (Data-encryptie) “TKIP” of “AES”. Deze instelling moet gelijk zijn aan die van de draadloze router of het draadloze accesspoint

6. Typ de encryptiesleutel in in het vakje naast “Network Key” (Netwerksleutel).

Belangrijk: Voer uw pre-shared sleutel in. Deze sleutel bestaat uit 8 tot 63 tekens, dit kunnen letters, cijfers of symbolen zijn. U dient bij al uw cliënten dezelfde sleutel te gebruiken.

7. Klik op “OK” om de instellingen op te slaan.

Wat is het verschil tussen 802.11b, 802.11g, G+ MIMO en Pre-N?

Op dit moment zijn er vier standaarden voor draadloze netwerken, waartussen grote verschillen in overdrachtssnelheden bestaan. Elke norm is gebaseerd op de aanduiding 802.11(x), een benaming die is vastgesteld door het IEEE (Institute of Electrical and Electronic Engineers), het Amerikaanse instituut dat verantwoordelijk is voor de ontwikkeling en goedkeuring van ondermeer netwerknormen. De meest gebruikte standaard voor draadloos netwerkverkeer is 802.11b. Deze maakt een gegevensoverdracht van 11 Mbps mogelijk. De standaarden 802.11a en 802.11g maken snelheden tot 54 Mbps mogelijk. G+ MIMO werkt eveneens met snelheden tot 54 Mbps en Pre-N met snelheden tot 108 Mbps.

Vergelijkend overzicht van draadloze technologieën

Draadloze technologie	802.11b	G (802.11g)	G+ (802.11g met HSM)	G+ MIMO(802.11g met MIMO MRC)	Belkin Pre-N (802.11g met TrueMIMO)
Snel-heid*	11Mbps-verbindingssnelheid/ basislijn	5x sneller dan 802.11b*	10x sneller dan 802.11b*	10x sneller dan 802.11b*	15x sneller dan 802.11b*
Frequentie	De vrije 2,4GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons	De vrije 2,4GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons	De vrije 2,4GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons	De vrije 2,4GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons	De vrije 2,4GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons
Compatibiliteit	Compatibel met 802.11g	Compatible met 802.11b/g	Compatibel met 802.11b/g	Compatibel met 802.11b/g	Compatibel met 802.11g en 802.11b
Bereik*	Doorgaans 30–60 m binnenshuis	Tot 120 m*	Tot 210 m*	Tot 300 m*	Tot 425 m*
Voordeel	Algemeen aanvaard	Veel gebruikt – vooral voor het delen van internetaansluitingen	Groter bereik en hogere snelheden	Betere dekking en constante snelheden	Geavanceerd – beste reikwijdte en doorvoer

*Bereik en verbindingssnelheid afhankelijk van netwerkomgeving.

Appendix A: Verklarende woordenlijst

IP Address (IP-adres)

Het “IP address” is het interne IP-adres van de router. Om de geavanceerde installatie-interface te openen, moet u dit adres in de adresbalk van uw browser typen. U kunt dit adres indien nodig wijzigen. Om het IP-adres te wijzigen, typt u het nieuwe IP-adres in en klikt u op “Apply Changes” (Wijzigingen aanbrengen). Het IP-adres dat u kiest, moet een niet-routeerbaar IP zijn. Hieronder ziet u een paar voorbeelden van een niet-routeerbaar IP:

192.168.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)

10.x.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)

Subnet Mask (Subnetmasker)

Sommige netwerken zijn veel te groot om, waardoor niet al het verkeer in alle uithoeken terecht komt. Deze netwerken moeten worden opgedeeld in kleinere, werkbare delen, subnets genaamd. Het subnetmasker is het netwerkadres plus de informatie die identificatie van het “subnetwerk” mogelijk maakt.

DNS

DNS staat voor Domain Name Server. Een "Domain Name Server" is een server op het Internet die URL's (Universal Resource Links) als "www.belkin.com" vertaalt naar IP-adressen. De meeste ISP's verlangen niet van u dat u deze informatie in de router invoert. Als u een statisch IP gebruikt, moet u waarschijnlijk een specifiek DNS-adres en een secundair DNS-adres invullen om ervoor te zorgen dat uw verbinding correct functioneert. Als u een dynamische verbinding of PPPoE gebruikt, hoeft u waarschijnlijk geen DNS-adres in te vullen.

PPPoE

De meeste ADSL-providers maken gebruik van PPPoE als type verbinding. Als u gebruik maakt van een ADSL-modem voor het maken van een verbinding met het Internet, dan gebruikt uw ISP mogelijk PPPoE om u aan te melden.

Uw type verbinding is PPPoE als:

1. uw ISP u een gebruikersnaam en een wachtwoord heeft gegeven die noodzakelijk zijn om de verbinding met het internet tot stand te brengen.
2. uw provider u software als WinPoET of Enternet300 heeft verstrekt om de internetverbinding tot stand te brengen.
3. u op een ander desktoppictogram dan uw browser moet dubbelklikken om op Internet te kunnen.

   Om de router geschikt te maken voor het gebruik van PPPoE, moet u uw gebuikersnaam en wachtwoord invoeren in de daarvoor bestemde velden. Nadat u alle noodzakelijke informatie hebt ingevoerd, klikt u op "Apply Changes" (Wijzigingen aanbrengen).

Nadat u de noodzakelijke wijzigingen hebt aangebracht, geeft de internetstatusindicator de melding "Connection OK" (Verbinding OK), als uw router correct is geïnstalleerd.

PPPoA

Voer de PPPoA-informatie in de daarvoor bestemde ruimtes en klik op "Next" (Volgende). Klik op "Apply" (Toepassen) om de instellingen te activeren.

1. User name (Gebruikersnaam) - Voer de gebruikersnaam in. (Toegekend door uw ISP).
2. Password (Wachtwoord) - Voer uw wachtwoord in. (Toegekend door uw ISP).
3. Retype Password (Wachtwoord opnieuw intypen) - Typ het wachtwoord opnieuw in (Toegekend door uw ISP).

4. VPI/VCI - Voer de paramters voor de Virtual Path Identifier (VPI) en de Virtual Circuit Identifier (VCI) in. (Toegekend door uw ISP).

Verbinding verbreken na X...

Deze functie wordt gebruik om automatisch de verbinding van uw router met het internet te verbreken als er gedurende bepaalde tijd geen activiteit is. Als u bijvoorbeeld deze optie aanvinkt en het cijfer 5 in het minutenveld invult, wordt de verbinding van de router met het Internet automatisch verbroken als er gedurende vijf minuten geen Internetactiviteit is geweest. Gebruik deze optie als u voor gebruik van het internet per tijdseenheid moet betalen.

Kanaal en SSID

U kunt het kanaal waarvan de router gebruik maakt, wijzigen door in het dropdown-menu het gewenste kanaal te kiezen en het gewenste kanaal te selecteren. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan. U kunt ook de SSID wijzigen. De SSID is het equivalent van de naam van uw draadloze netwerk. U kunt de SSID elke naam geven die u wilt. Als er meer draadloze netwerken in uw omgeving actief zijn, geef uw draadloze netwerk dan een unieke naam. Klik in het SSID-vak en typ een nieuwe naam in. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijzigingen door te voeren.

Gebruik maken van de ESSID Broadcast-functie

Veel draadloze netwerkadapters die momenteel op de markt verkrijgbaar zijn, beschikken over een functie genaamd site survey. Deze functie scant naar beschikbare netwerken en stelt elke computer in staat automatisch een netwerk uit de survey te selecteren. Dit gebeurt als de SSID van de computer is ingesteld op “ANY”. Uw router van Belkin kan deze willekeurige zoektocht naar een netwerk blokkeren. Indien u de “ESSID Broadcast”-functie uitschakelt, kan een computer het netwerk alleen vinden als u de SSID van de computer op de specifieke naam van het netwerk (zoals WLAN) instelt. Zorg er wel voor dat u uw SSID (netwerknaam) kent voordat u deze functie inschakelt. U kunt uw draadloze netwerk zo goed als onzichtbaar maken. Wanneer u de optie SSID-uitzending uitschakelt, verschijnt het netwerk niet in site-overzichten. Door het uitschakelen van de SSID-uitzending, helpt u de veiligheid te verhogen.

Encryptie

Door het gebruik van encryptie zorgt u voor een betere beveiliging van uw netwerk. De router maakt gebruik van Wired Equivalent Privacy (WEP) en WIFI Protected Access (WPA) om uw gegevens te beschermen en biedt twee encryptiemogelijkheden: 64-bits en 128-bits encryptie. Encryptie werkt met een sleutelsysteem. De sleutel op de computer moet overeen komen met de sleutel van de router. Er zijn twee manieren om een sleutel te creëren. Bij de

eenvoudigste methode laat u de router's software een passphrase (meervoudig wachtwoord) converteren naar een sleutel. Een geavanceerde methode is het handmatig invoeren van de sleutels.

Virtuele servers

De functie Virtuele Servers biedt u de mogelijkheid externe (internet)verbindingen voor diensten zoals een webserver (poort 80), FTP-server (poort 21), of andere applicaties, via uw router door te sturen naar uw interne netwerk. Aangezien uw interne computers beschermd worden door een firewall, kunnen computers buiten uw netwerk (via het Internet) de interne computers niet bereiken omdat ze niet "zichtbaar" zijn. Als u de functie "virtual server" voor een specifieke applicatie dient te configureren, neem dan contact op met de leverancier van de applicatie om geïnformeerd te worden over welke poortinstellingen u nodig hebt.

Om instellingen handmatig in te voeren, typt u het IP-adres in het vak voor de interne computer in, geeft u het poortype (TCP of UDP) op en de LAN- en publieke poort(en) die gepasseerd moeten worden. Selecteer vervolgens "Enable" (Activeren) en klik op "Set" (Instellen). U kunt per intern IP-adres slechts één poort vrijgeven. U neemt een zeker risico door poorten in uw firewall te openen. U kunt instellingen zeer snel in- en uitschakelen. Wij adviseren deze instellingen uit te schakelen wanneer u een bepaalde toepassing niet gebruikt.

Cliënt IP-filters

De router kan zo worden geconfigureerd dat toegang tot het Internet, e-mail, of andere netwerkdiensten op bepaalde dagen en tijden beperkt is. Deze beperking kan worden ingesteld voor één computer, een groep computers of verschillende computers.

MAC-adressenfilter

Het MAC-adressenfilter is een krachtig beveiligingsinstrument waarmee u kunt aangeven welke computers toegang hebben tot het netwerk. Elke computer die probeert het netwerk binnen te komen maar die niet in de filterlijst voorkomt, wordt de toegang geweigerd. Wanneer u deze functie activeert, moet u het MAC-adres invoeren van iedere cliënt op uw netwerk om elk van deze cliënten toegang te geven tot het netwerk. U kunt ook het MAC-adres kopiëren door de naam van de computer te selecteren in het "DHCP Client List"-overzicht. Om deze functie te activeren, selecteert u "Enable" (Activeren). Klik vervolgens op "Apply Changes" (Wijzigingen aanbrengen) om de instellingen op te slaan.

DMZ

Indien een van uw cliënten van achter de firewall geen internetapplicatie kan draaien, kunt u deze cliënt onbeperkte tweewegs internettoegang verstrekken. Dit kan nodig zijn wanneer de NAT-functie problemen veroorzaakt met applicaties als games en videoconferenties. Schakel deze functie alleen tijdelijk in. **Computers in de gedemilitariseerde zone zijn niet tegen hackeraanvallen beveiligd.** Om een computer in de gedemilitariseerde zone te plaatsen, dient u het LAN IP-adres van deze computer in het “Static IP”-veld in te vullen en te klikken op “Apply Changes” (Wijzigingen aanbrengen).

Als u slechts een publiek (WAN) IP-adres hebt, kunt u het publieke IP laten staan op “0.0.0.0”. Als u meerdere publieke WAN IP-adressen gebruikt, kunt u aangeven op welk publiek WAN IP-adres de DMZ-host gericht zal zijn. Vul het (WAN) IP-adres in waaraan de DMZ-host moet worden gericht, voer de laatste twee cijfers in van het IP-adres van de DMZ-hostcomputer en klik op “Apply Changes” (Wijzigingen aanbrengen).

Beheerderswachtwoord

De router wordt geleverd ZONDER vooraf geprogrammeerd wachtwoord. Als u een wachtwoord wilt toevoegen voor meer beveiliging, dan kunt u via de web-based gebruikersinterface van uw router een wachtwoord instellen. Bewaar uw wachtwoord op een veilige plek, want u zal het nodig hebben als u in de toekomst op de router wilt inloggen. Wij raden u **TEN ZEERSTE** aan een wachtwoord in te stellen als u van plan bent de functie “beheer op afstand” van uw router te gebruiken Met de optie inlog-timeout kunt u de maximale tijdsduur instellen waarbinnen u ingelogd kunt blijven op de Advanced Setup Interface (Geavanceerde setup-interface) van de router. De tijdklok begint te lopen als er geen activiteit is geweest. U hebt bijvoorbeeld een aantal wijzigingen in de geavanceerde gebruikersinterface aangebracht en daarna uw computer alleen gelaten zonder op “Logout” (Afmelden) te klikken.

Als de timeout is ingesteld op 10 minuten, dan loopt de inlogsessie af 10 minuten nadat u de router alleen hebt gelaten. Als u meer wijzigingen wilt aanbrengen, dient u opnieuw op de router in te loggen. Deze inlog-timeoutoptie is bedoeld als extra beveiliging en staat standaard ingesteld op 10 minuten. Let op: er kan slechts één computer tegelijk ingelogd zijn op de Advanced Setup-interface van de router.

Tijd en tijdzone

De tijdklok van de router wordt geregeld via de aansluiting op een SNTP (Simple Network Time Protocol) server. Hierdoor loopt de systeemklok van de router synchroon met de tijd van het wereldwijde internet. De gesynchroniseerde klok in de router wordt gebruikt voor de registratie van de beveiligingslog en de aansturing van het cliëntenfilter. Selecteer de tijdzone waarin u gevestigd bent. Als u in een land woont dat de zomer- en wintertijd volgt, vink dan de optie “Enable Daylight Saving” (Zomer/wintertijd inschakelen) aan. De systeemklok geeft niet onmiddellijk na inschakeling de juiste tijd aan. De router heeft ten minste 15 minuten nodig om een verbinding op te bouwen met de tijdservers op het Internet en voor het ontvangen van een antwoordsignaal.

Beheer op afstand

ZORG ERVOOR DAT U HET BEHEERDERSWACHTWOORD HEBT INGESTELD, voordat u deze functie inschakelt.. De functie “Remote Management” (Beheer op afstand) biedt u de mogelijkheid vanaf elke internetlocatie ter wereld de instellingen van uw router te wijzigen.

UPnP

UPnP (Universal Plug-and-Play is een technologie die naadloze werking van voice messaging, video messaging, games en andere applicaties mogelijk maakt die voldoen aan UPnP. Voor sommige applicaties dient de firewall van de router op een specifieke manier geconfigureerd te zijn voor een juiste werking. Hiervoor moeten doorgaans de TCP- en UDP-poorten worden geopend en in sommige gevallen triggerpoorten worden ingesteld. Applicaties die voldoen aan UpnP kunnen met de router communiceren, in principe om de router te “vertellen” op welke wijze de firewall moet worden geconfigureerd. Bij aflevering is de UPnP-functie van de router uitgeschakeld. Als u applicaties gebruikt die voldoen aan UpnP en u wilt profiteren van de mogelijkheden van UPpnP dan heeft het zin de UPnP-functie te activeren. U selecteert eenvoudigweg “Enable” (Activeren) in de paragraaf “UPnP Enabling” (UPnP activeren) van de pagina “Utilities” (Hulpprogramma’s). Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijziging op te slaan.

Appendix B: Belangrijke factoren die een rol spelen bij plaatsing en setup

Let op: Hoewel de onderstaande factoren de prestaties van een netwerk nadelig kunnen beïnvloeden, beletten zij niet dat het draadloze netwerk functioneert. Als u denkt dat het netwerk niet optimaal presteert, kan deze checklist uitkomst bieden.

1. **Plaatsing van uw draadloze router (of draadloos accesspoint)**

   Plaats uw draadloze router (of accesspoint), het centrale verbindingspunt binnen uw netwerk, op een centrale plek tussen uw draadloze netwerkapparatuur.

   De beste netwerkdekking voor uw “draadloze cliënten” (d.w.z. computers aangestuurd door draadloze notebook- en desktopnetwerkkaarten en draadloze USB-adapters van Belkin) bereikt u als volgt:

   - Zorg ervoor dat de netwerkantennes van uw draadloze router (of accesspoint) parallel aan elkaar en in verticale stand staan (naar het plafond wijzen). Als de draadloze router (of het draadloze accesspoint) zelf al verticaal is gepositioneerd, laat de antennes dan zo recht mogelijk naar het plafond wijzen.
   - In woningen met meer verdiepingen plaatst u de draadloze router (of het draadloze accesspoint) op de verdieping die zich het dichtst bij het midden van de woning bevindt. Dit kan betekenen dat u de draadloze router (of het draadloze accesspoint) op een hogere verdieping moet plaatsen.
   - Plaats de draadloze router (of het draadloze accesspoint) niet in de buurt van een draadloze 2,4GHz-telefoon.

2. **Vermijd obstakels en interferentie**

   Plaats uw draadloze router (of accesspoint) bij voorkeur niet in de buurt van apparaten die radiogolven uitzendt, zoals magnetrons De volgende ondoordringbare objecten kunnen draadloze communicatie hinderen:

   - Koelkasten
   - Wasmachines en/of drogers
   - Metalen kasten
   - Grote aquaria
   - Gemetalliseerde UV-werende ruiten

Indien het signaal van uw draadloze netwerk op sommige plaatsen zwakker lijkt te zijn, zorg er dan voor dat dit soort objecten het signaal niet kunnen hinderen, dat wil zeggen dat ze niet tussen uw computers en uw draadloze router (of accesspoint) in staan.

3. **Draadloze telefoons**

Ga als volgt te werk als de prestaties van het draadloze netwerk niet beter worden nadat u de bovenstaande wenken hebt opgevolgd én u een draadloze telefoon bezit:

- Kijk wat er gebeurt als u uw draadloze telefoon uit de buurt houdt van uw draadloze router (of accesspoint) en uw computers die geschikt zijn voor draadloze communicatie.
- Verwijder de batterij uit alle draadloze telefoons die gebruik maken van de 2,4GHz-band (zie informatie van de fabrikant). Als het probleem hiermee is opgelost, is/zijn uw telefoon(s) de storingsbron.
- Als u voor uw telefoon ook andere kanalen kunt kiezen, kies dan voor het kanaal dat het verst verwijderd is van het kanaal dat door uw draadloze netwerk gebruikt wordt. Verander bijvoorbeeld het kanaal van uw telefoon in kanaal 1 en stel het kanaal van uw draadloze router (of accesspoint) in op kanaal 11. Raadpleeg de handleiding van uw telefoon voor gedetailleerde instructies.
- Ga zo nodig over op een draadloze telefoon van 900 MHz of 5 GHz.

4. **Kies het “stilste” kanaal voor het draadloze netwerk**

Op plaatsen waar meerdere woningen of kantoren dicht bij elkaar liggen, zoals appartementen- of kantoorgebouwen, kunnen draadloze netwerken in de omgeving problemen veroorzaken voor uw netwerk.

Maak gebruik van de Site Survey-mogelijkheid (site-overzicht) van de Wireless LAN Utility (hulpprogramma voor draadloos LAN) om andere draadloze netwerken te lokaliseren en verplaats uw router en computers naar een kanaal dat zo ver mogelijk verwijderd is van andere netwerken.

Experimenteer met de verschillende beschikbare kanalen om de beste verbinding te vinden en storing door draadloze telefoons en andere draadloze apparaten in de omgeving te voorkomen.

Gebruik voor niet van Belkin afkomstige draadloze netwerkproducten het gedetailleerde site-overzicht en de informatie over draadloze

kanalen in de handleiding.

Bovenstaande suggesties en richtlijnen helpen u bij het optimaliseren van het bereik van uw draadloze router (of accesspiont). Als u een nog groter bereik nodig hebt, overweeg dan de aanschaf van een draadloze range extender/accesspoint van Belkin.

5. Veilige verbindingen, VPN's en AOL.

Veilige verbindingen zijn verbindingen waarvoor een gebruikersnaam en een wachtwoord vereist zijn. Hiervan wordt gebruik gemaakt in situaties waar beveiliging van belang is. Veilige verbindingen zijn ondermeer:

- Virtual Private Network (VPN)-verbindingen; deze worden vaak gebruikt om van afstand verbinding te maken met een kantoornetwerk
- Het "Bring Your Own Access"-programma van America Online (AOL) - dit programma laat u AOL gebruiken via breedband die ter beschikking wordt gesteld door een andere kabel- of DSL-service.
- De meeste websites voor internetbankieren
- Veel commerciële websites waarbij toegang uitsluitend verleend wordt nadat een gebruikersnaam en wachtwoord zijn ingevuld

Veilige verbindingen kunnen worden onderbroken als het energiebeheer van de computer de computer naar de slaapstand overschakelt. U kunt opnieuw verbinding maken door de VPN of AOL-software te draaien, of door opnieuw op de beveiligde website in te loggen.

Een tweede alternatief is het veranderen van de energiebeheerinstelling en van de computer, zodat deze niet overgaat op de slaapstand. Dit is niet noodzakelijkerwijs van toepassing voor draagbare computers. Om de energiebeheerinstellingen te wijzigingen in Windows, gaat u naar "Power Options" (Energiebeheer) in het "Control Panel" (Configuratiescherm).

Indien u moeilijkheden blijft hebben met de beveiligde verbindingen, VPN's en AOL, loop de hierboven beschreven stappen dan door om te zien of u hiermee rekening gehouden hebt.

Appendix C: Overzicht met internet-verbindingsinstellingen

De tabel op de volgende pagina helpt u bij het selecteren en configureren van een ADSL-internetverbinding Veel ISP's maken gebruik van per regio verschillende instellingen en apparatuur. Probeer de instellingen voor de ISP's in uw regio. Als dit niet werkt, neem dan contact op met uw ISP en vraag naar uw specifieke instellingen.

Land	Verbindings-protocol	VPI/VCI	Encapsulatie	ISP's
Europa				
Frankrijk	PPPoE	8/35	LLC	Meerdere
Duitsland	PPPoE	1/32	LLC	T-Online, meerdere
Nederland	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Meerdere
België	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italië	PPPoE of PPPoA	8/35	VC MUX	TIN
Spanje	PPPoE of 1483 Bridged	8/32	LLC	Telefonica
Zweden	1483 Bridged	3/35	LLC	Telia
UK	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Azië				
Australië	PPPoE of PPPoA	8/35	LLC	Meerdere
Nieuw-Zeeland	PPPoE of PPPoA	0/100	VC MUX	Meerdere
Singapore	PPPoE	0/100	LLC	SingNet, Pacific Internet

FCC-verklaring

VERKLARING VAN CONFORMITEIT MET DE FCC-VOORSCHRIFTEN VOOR ELEKTROMAGNETISCHE COMPATIBILITEIT

Wij, Belkin Corporation, gevestigd 501 West Walnut Street, Compton, CA 90220, Verenigde Staten van Amerika, verklaren hierbij dat wij de volledige verantwoordelijkheid aanvaarden dat het product met het artikelnummer:

F5D9630-4

waarop deze verklaring betrekking heeft, voldoet aan Deel 15 van de FCC-voorschriften. Het gebruik ervan is onderworpen aan de beide volgende voorwaarden: (1) het apparaat mag geen schadelijke storingen opwekken en (2) het apparaat moet elke ontvangen interferentie accepteren, waaronder storingen die een ongewenste werking kunnen veroorzaken.

Waarschuwing: Blootstelling aan radiofrequente straling.
Het uitgangsvermogen van dit apparaat ligt ver beneden de hiervoor in de FCC-voorschriften vastgelegde grenswaarden voor stralingsfrequenties. Niettemin moet dit apparaat zo worden gebruikt dat onder normale omstandigheden de mogelijkheid van persoonlijk contact tot een minimum beperkt blijft.

Ook bij het aansluiten van een externe antenne op dit apparaat moet de antenne zodanig worden geplaatst dat bij normaal gebruik de kans op aanraking tot een minimum beperkt blijft. Ter voorkoming overschrijding van de in de FCC-voorschriften aangegeven grenswaarden voor de blootstelling aan radiofrequente straling, mogen personen de werkende antenne niet dichter naderen dan tot op een afstand van 20 centimeter.

Kennisgeving van de Federal Communications Commission (FCC)
Deze apparatuur is getest en voldoet aan de grenswaarden voor digitale apparaten van Klasse B zoals vastgelegd in Deel 15 van de FCC-voorschriften. Deze normen zorgen bij de installatie in een woonomgeving voor een aanvaardbare bescherming tegen schadelijke interferentie.

Deze apparatuur genereert en gebruikt radiofrequente energie en kan deze tevens uitzenden. Als deze apparatuur de radio- of televisie-ontvangst stoort, wat u kunt vaststellen door de apparatuur in- en uit te schakelen, kunt u proberen de storing op te heffen met een of meer van de volgende maatregelen:

- Draai de ontvangende antenne in een andere richting of zet de antenne op een andere plaats.
- Door het vergroten de afstand tussen de apparatuur en de ontvanger.
- Sluit de apparatuur aan op een stopcontact van een andere groep dan die waarop de ontvanger is aangesloten.
- Neem contact op met de verkoper of een deskundig radio/ televisietechnicus.

Veranderingen

De Federal Communications Commission eist dat de gebruiker wordt gewaarschuwd dat elke verandering aan het apparaat die niet uitdrukkelijk door Belkin Corporation is goedgekeurd de bevoegdheid van de gebruiker om het apparaat te bedienen teniet kan doen.

Canada-Industry Canada (IC)

De draadloze radio van dit apparaat voldoet aan RSS 139 & RSS 210 Industry Canada. This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Kennisgeving betreffende de Europese Unie

Radioproducten die voorzien zijn van de CE 0560- of de CE-aanduiding voldoen aan de R&TTE-richtlijn (1995/5/EC) van de Commissie van de Europese Gemeenschap.

Het voldoen aan deze richtlijn houdt in dat de betreffende apparatuur beantwoordt aan de volgende Europese normen (de overeenkomstige internationale normen zijn tussen haakjes vermeld).

- EN 60950 (IEC60950) – Productveiligheid
- EN 300 328 Technische vereisten voor radioapparatuur
- ETS 300 826 - Algemene vereisten voor radioapparatuur wat betreft elektromagnetische compatibiliteit.

U kunt het zendertype vaststellen op het identificatie-etiket van uw apparaat van Belkin.

Producten die voorzien zijn van het CE-merk voldoen aan de Richtlijn voor Elektromagnetische Compatibiliteit (89/336/EEC) en aan de Richtlijn voor Laagspanningsapparatuur (72/23/EEC) van de Commissie van de Europese Economische Gemeenschap. Apparaten die aan deze richtlijn voldoen beantwoorden aan de volgende Europese normen (tussen haakjes zijn de overeenkomstige internationale normen vermeld).

- EN 55022 (CISPR 22) – Elektromagnetische interferentie
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Elektromagnetische immuniteit
- EN 61000-3-2 (IEC610000-3-2) – Harmonischen in elektrische leidingen
- EN 61000-3-3 (IEC610000) – Spanningsfluctuaties in elektrische leidingen
- EN 60950 (IEC60950) – Productveiligheid

Producten die een radiozender bevatten zijn voorzien van het CE 0560- of CE-waarschuwingsmerk en kunnen tevens zijn voorzien van het CE-logo.



Dit symbool op het product of de verpakking geeft aan dat dit product niet mag worden afgevoerd met het huishoudelijk afval. Het is uw verantwoordelijkheid uw afgedankte apparatuur af te leveren op een aangewezen inzamelpunt voor de verwerking van afgedankte elektrische en elektronische apparatuur. De gescheiden inzameling en verwerking van uw afgedankte apparatuur draagt bij tot het sparen van natuurlijke bronnen en tot het hergebruik van materiaal op een wijze die de volksgezondheid en het milieu beschermt. Voor meer informatie over waar u uw afgedankte apparatuur kunt inleveren voor recycling kunt u contact opnemen met het gemeentehuis in uw woonplaats, de reinigingsdienst of de winkel waar u het product hebt aangeschaft.

Beperkte levenslange productgarantie van Belkin Corporation

Belkin Corporation geeft garantie voor de levensduur van het product op materiaal- en fabricagefouten. Wanneer een defect wordt geconstateerd, zal Belkin naar eigen keuze het product repareren of kosteloos vervangen, op voorwaarde dat het product tijdens de garantieperiode, met vooruitbetaalde vervoerskosten, wordt geretourneerd aan de officiële Belkin dealer bij wie het product is gekocht. Overlegging van het aankoopbewijs kan noodzakelijk zijn.

Deze garantie is niet van toepassing als het product is beschadigd als gevolg van een ongeluk, misbruik, verkeerd gebruik of een verkeerde toepassing; als het product zonder schriftelijke toestemming van Belkin is gewijzigd of als een serienummer dat door Belkin is aangebracht, is verwijderd of onleesbaar is gemaakt.

DE GARANTIE EN VERHAALSMOGELIJKHEDEN DIE HIERVOOR ZIJN UITEENGEZET SLUITEN ELKE ANDERE GARANTIE OF VERHAALSMOGELIJKHEID UIT, HETZIJ MONDELING OF SCHRIFTELIJK, HETZIJ UITDRUKKELIJK OF IMPLICIET. BELKIN WIJST UITDRUKKELIJK ELKE EN ALLE IMPLICIETE AANSPRAKELIJKHEID OF GARANTIE AF, WAARONDER, ZONDER ENIGE BEPERKING, GARANTIES BETREFFENDE DE VERKOOPBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALDE TOEPASSING.

Geen enkele dealer, vertegenwoordiger of werknemer van Belkin is bevoegd tot wijziging, uitbreiding of aanvulling van deze garantie.

BELKIN IS NIET AANSPRAKELIJK VOOR SPECIFIEKE SCHADE, INCIDENTELE SCHADE OF GEVOLGSCHADE TEN GEVOLGE VAN HET NIET NAKOMEN VAN DE GARANTIEVOORWAARDEN OF TEN GEVOLGE VAN ENIG ANDER JURIDISCH CONFLICT, WAARONDER BEGREPEN WINSTDERVING, PRODUCTIETIJDVERLIES, GOODWILL, BESCHADIGING VAN PROGRAMMA'S OF GEGEVENS DIE ZIJN OPGESLAGEN IN OF WORDEN GEBRUIKT DOOR BELKIN-PRODUCTEN, EN HET OPNIEUW PROGRAMMEREN OF REPRODUCEREN ERVAN.

In sommige staten of landen is het niet toegestaan om incidentele schade, voortvloeiende schade en impliciete garanties uit te sluiten of te beperken; in dat geval gelden de bovenstaande beperkingen of uitsluitingen wellicht niet voor u. Deze garantie verleent u specifieke wettelijke rechten en wellicht hebt u andere rechten die van staat tot staat verschillen.

ADSL2+ modem met ingebouwde draadloze G+ MIMO router

Aanvullende informatie over technische ondersteuning is beschikbaar op www.belkin.com onder “Ondersteuning”.
“Indien u telefonisch* contact wilt opnemen met onze afdeling voor technische ondersteuning, kunt u gebruik maken van het voor u van toepassing zijnde telefoonnummer uit onderstaande lijst. Onze afdeling voor technische ondersteuning is bereikbaar tijdens kantooruren.”

*Tegen standaard telefoontarief

Gratis technische ondersteuning*

OOSTENRIJK	08 - 20 20 07 66
TSJECHIË	23 900 04 06
DENEMARKEN	701 22 403
FINLAND	00800 - 22 35 54 60
FRANKRIJK	08 - 25 54 00 26
DUITSLAND	0180 - 500 57 09
GRIEKENLAND	00800 - 44 14 23 90
HONGARIJE	06 - 17 77 49 06
IJSLAND	800 8534
IERLAND	0818 55 50 06
ITALIË	02 - 69 43 02 51
LUXEMBURG	34 20 80 8560
NEDERLAND	0900 - 040 07 90
NOORWEGEN	815 00 287
POLEN	00800 - 441 17 37
PORTUGAL	707 200 676
RUSLAND	495 580 9541
ZUID-AFRIKA	0800 - 99 15 21
SPANJE	902 - 02 43 66
ZWEDEN	07 - 71 40 04 53
ZWITSERLAND	08 - 48 00 02 19
UK	0845 - 607 77 87

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Verenigd Koninkrijk
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin Ltd.
7 Bowen Crescent, West Gosford
NSW 2250, Australië
+61 (0) 2 4372 8600
+61 (0) 2 4372 8603 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Nederland
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

P75125ea_A

BELKIN

Módem ADSL2+ con router inalámbrico G+ MIMO

Conecte en red a sus ordenadores y comparta su acceso ADSL a Internet

UK

FR

DE

NL

ES

IT



Manual del usuario

802.11g
G+
MIMO

F5D9630sp4A

Índice de contenidos

Gracias por la adquisición del Módem ADSL con router inalámbrico G con modo de alta velocidad (en adelante, el router). En pocos minutos podrá compartir su conexión a Internet y establecer una red entre sus ordenadores con su nuevo router. A continuación presentamos una lista de características que convierten su nuevo router en la solución ideal para su red de oficina pequeña o del hogar. Lea atentamente el presente manual del usuario y preste especial atención al Anexo B titulado “Factores importantes para la colocación y configuración”.

Ventajas de una red de hogar

Siguiendo nuestras sencillas instrucciones de instalación, podrá utilizar su red del hogar de Belkin para:

- Compartir una conexión de Internet de alta velocidad con todos los ordenadores de su hogar
- Compartir recursos, como archivos y discos duros, entre todos los ordenadores conectados en su hogar
- Compartir una única impresora con toda la familia
- Compartir documentos, música, vídeo e imágenes digitales
- Almacenar, recuperar y copiar archivos de un ordenador a otro
- Participar en juegos on-line de forma simultánea, consultar su correo electrónico y chatear

Ventajas de una red inalámbrica de Belkin

Movilidad: ya no necesitará una sala dedicada exclusivamente al almacenamiento de ordenadores; ahora podrá trabajar en cualquier parte dentro de su alcance inalámbrico con un ordenador de sobremesa o portátil conectado en red

Instalación sencilla – el Asistente de Instalación Sencilla de Belkin facilita la instalación

Flexibilidad: instale y acceda a impresoras, ordenadores y otros dispositivos de red desde cualquier punto de su hogar

Fácil de ampliar: la extensa gama de productos de interconexión en red de Belkin le permite ampliar su red para incluir dispositivos adicionales, como impresoras y videoconsolas de juegos

Sin necesidad de cableado: podrá ahorrarse los gastos y las complicaciones de colocar cableado Ethernet por toda su casa u oficina

Aceptación general en el sector: seleccione entre una amplia gama de productos de interconexión en red compatibles

Asegúrese de tener los siguientes elementos al alcance de la mano

Contenido del paquete

- Módem ADSL2+ con router inalámbrico G+ MIMO
- Cable de teléfono RJ11 (de color gris)
- Cable de red Ethernet RJ45 (de color amarillo)
- Microfiltro ADSL*
- Adaptador de corriente
- Manual del usuario en CD

*El microfiltro ADSL varía según el país. Si éste no está incluido, necesitará adquirir uno.

Requisitos del sistema

- Un servicio ADSL activo con un enchufe de pared para el teléfono para conectar el router
- Al menos un ordenador con una tarjeta de interfaz de red (NIC, Network Interface Card) y un navegador de Internet instalado y configurado correctamente
- Protocolo de red TCP/IP instalado en todos los ordenadores conectados al router
- Ningún otro servidor de su red local debe asignar las direcciones IP a ordenadores y dispositivos

Ajustes para la conexión a Internet

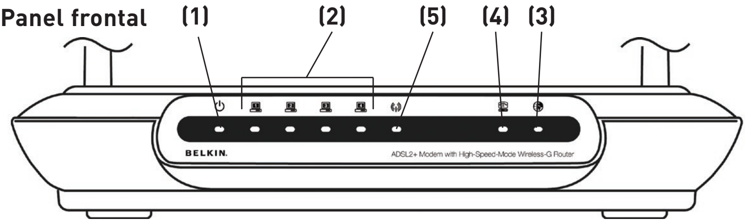
Solicite a su Proveedor de Servicios de Internet, ISP, la siguiente información antes de configurar el Módem ADSL con router inalámbrico G.

- Protocolo de conexión a Internet ________ (PPPoE, PPPoA, IP dinámica, IP estática)
- Método múltiplex o encapsulamiento: _________ (LLC o VC MUX)
- Circuito virtual: VPI (identificador de ruta virtual) _________
  (un número entre 0 y 255)
- VCI (Identificador virtual de canal) _________
  (un número entre 1 y 65535)
- Para usuarios PPPoE y PPPoA: Cuenta de usuario ADSL ____________ y contraseña ______________
- Para usuarios de IP estática: Dirección IP.___ . ___ . ___ . ___
  Máscara de subred ___ . ___ . ___ . ___
  Servidor de Pasarela por defecto ___ . ___ . ___ .
- Dirección IP para el Servidor de nombres de dominio ___ . ___ . ___ .___
  (si hasidosuministrado por su ISP)

Atención: En el anexo C de este manual del usuario encontrará algunos de los parámetros más frecuentes para Internet DSL. Si tiene dudas, consulte a su ISP.

El router ha sido diseñado para su colocación sobre un escritorio. Todos los cables salen de la parte posterior del router para lograr una mejor organización y utilidad. Los indicadores LED se encuentran fácilmente visibles en la parte frontal del router para proporcionarle información acerca de la actividad y el estado de la red.

Panel frontal



1. LED de Encendido

Cuando enciende la alimentación del router o lo reinicia, transcurre un breve período de tiempo mientras arranca el router. Cuando el router haya arrancado por completo, el LED de Encendido se iluminará de forma VERDE indicando que el router está listo para ser utilizado.

	APAGADO	El router está APAGADO
	Verde	El router está ENCENDIDO
	Rojo	El router no ha podido arrancar

2. Indicadores LED de estado LAN

Estos indicadores LED presentan etiquetas con los números del 1 al 4 y corresponden a los puertos numerados en la parte posterior del router. Cuando un ordenador se encuentre correctamente conectado a uno de los puertos LAN de la parte posterior del Router, el LED se iluminará. VERDE permanente significa que un ordenador o un dispositivo en red están conectados. Cuando se esté enviando información a través del puerto, el LED parpadeará rápidamente. ÁMBAR indica una conexión 10Base-T.

	APAGADO	No hay ningún dispositivo conectado
	Naranja	La conexión Ethernet está activa y un dispositivo 10Base-T se encuentra conectado.
	Ámbar - parpadeante	Un dispositivo 10Base-T está transmitiendo o recibiendo datos
	Verde	La conexión Ethernet está activa y 100Base-T está conectado.
	Verde - parpadeante	Un dispositivo 100Base-T está transmitiendo o recibiendo datos

3. **Indicador LED de estado de WLAN**
El indicador LED de estado de WLAN está VERDE permanente cuando activa la función LAN inalámbrica. Parpadea cuando el router está transmitiendo o recibiendo datos de manera inalámbrica.

	APAGADO	WLAN está desactivado
	Verde	WLAN está funcionando y conectado
	Verde - parpadeante	Cuando se transmiten o reciben datos

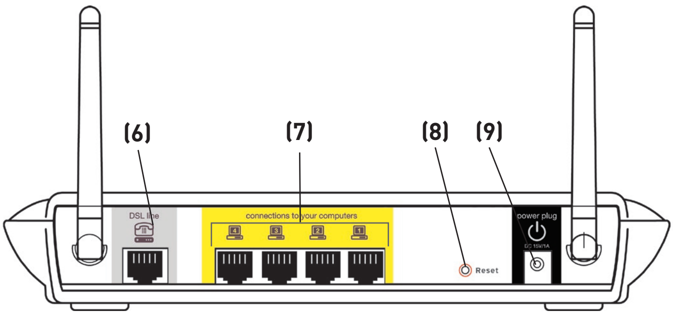
4. **Indicador LED de ADSL**
El indicador LED de ADSL se ilumina VERDE cuando está negociando con su ISP. Permanece VERDE cuando el router está conectado correctamente a su servicio de ADSL.

	APAGADO	No hay conexión ADSL
	Verde	El vínculo ADSL está funcionando y conectado
	Verde - parpadeante	gestionando la conexión

5. **Indicador LED de Internet**
El indicador LED de Internet le indica cuándo está conectado el router a Internet. Cuando la luz está APAGADA, el router NO está conectado a Internet. Cuando la luz es VERDE permanente, el router está conectado a Internet. Cuando el LED está parpadeante, el router está transmitiendo o recibiendo datos de Internet.

	APAGADO	No hay conexión a Internet
	Verde	Conectado a Internet
	Verde - intermitente	Cuando se transmiten o reciben datos
	Rojo	Error al intentar obtener la IP

Panel posterior



6. **Línea DSL**
   Este puerto sirve para conectar su línea ADSL. Conecte su línea ADSL a este puerto.

7. **Puertos Ethernet**
   Los puertos Ethernet son RJ45, 10/100, de negociación automática. Los puertos están marcados s con números del 1 al 4. Dichos puertos se corresponden con los indicadores LED numerados de la parte frontal del router. Conecte sus ordenadores de red o cualquier otro dispositivo de red a uno de estos puertos.

8. **Botón de reinicio**
   El botón de “Reset” (Reinicio) se emplea en casos excepcionales cuando el router puede estar funcionando mal. Al reiniciar el router se restablecerá el funcionamiento normal del mismo manteniendo los ajustes programados. También puede restablecer los ajustes por defecto de fábrica utilizando el botón de Reinicio. Emplee la función de restablecimiento en caso de que haya olvidado su contraseña personal.

   a. **Reinicio del router**
      Pulse y suelte el botón de reinicio. Cuando la luz de Encendido obtenga de nuevo un color permanente, el reinicio habrá sido completado.

   b. **Restablecimiento de los ajustes por defecto de fábrica**
      Pulse y mantenga pulsado el botón de Reinicio durante cinco segundos y suéltelo después. Cuando la luz de Encendido obtenga de nuevo un color permanente, el restablecimiento habrá sido completado.

9. **Toma de alimentación**
   Conecte a esta toma la fuente de alimentación de 15V CC adjunta. Si utiliza un adaptador de alimentación incorrecto, podrá causar daños irreversibles a su router.

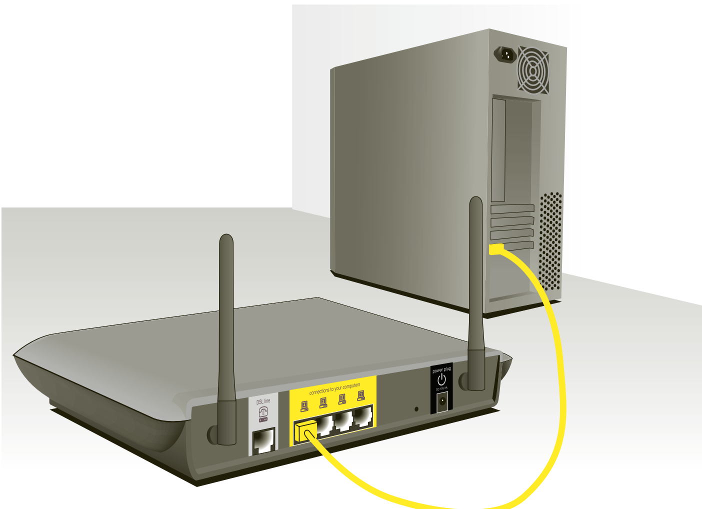
Colocación del router

Su conexión inalámbrica será más potente cuanto más cerca se encuentre el ordenador de su router. El alcance habitual de funcionamiento de sus dispositivos inalámbricos en interiores se sitúa entre los 30 y los 60 metros. De la misma forma, su conexión y rendimiento inalámbricos se verán algo mermados a medida que aumente la distancia entre los dispositivos conectados a su router inalámbrico y los dispositivos conectados. Puede que usted lo aprecie, aunque no necesariamente. Si se aleja aún más de su router, es posible que descienda su velocidad de conexión. Los factores que pueden debilitar las señales al interferir en el recorrido de las ondas de radio de su red, son los aparatos u obstáculos de metal y las paredes. Véase también el Anexo B: Factores importantes para la colocación y configuración" del presente manual del usuario.

Si está preocupado por un mal rendimiento de su red que pudiera estar relacionado con factores de alcance o de obstrucción, pruebe a desplazar el ordenador hasta una posición de 3 metros de distancia de su router inalámbrico con el fin de comprobar si el problema se debe a la distancia. Si las dificultades continúan a pesar de una distancia corta, consulte la sección de resolución de problemas.

Conexión de los ordenadores

1. Apague los ordenadores y el equipo de red.
2. Conecte su ordenador a uno de los puertos RJ45 AMARILLOS de la parte posterior del router, con la etiqueta “conexiones a los ordenadores”. Para ello, utilice un cable de red Ethernet (un cable de red Ethernet se encuentra incluido en el paquete).



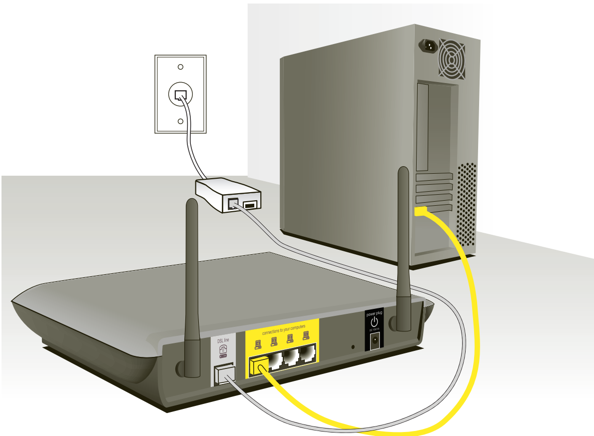
Conexión de la línea de ADSL

La conexión del router a la línea ADSL varía según el país o región. Normalmente se necesita un microfiltro o uno con un distribuidor incluido para permitir el uso simultáneo del servicio ADSL y del servicio telefónico en la misma línea de teléfono. Lea atentamente los siguientes pasos y seleccione el método apropiado.

1. Si sus servicios de teléfono y ADSL se encuentran en una misma línea de teléfono, necesitará un microfiltro ADSL para cada teléfono y cada otro dispositivo que utilice, como contestador automático y fax. Se pueden utilizar filtros adicionales para separar las líneas de teléfono en teléfono y router.

   Nota: No conecte el microfiltro ADSL entre la toma de pared y el router, ya que de esta manera, el servicio de ADSL no logrará alcanzar el módem.

2. Si sus servicios de teléfono y ADSL se encuentran en la misma línea de teléfono y usted está utilizando un microfiltro ADSL con un divisor de línea incorporado, conecte el divisor a la toma de teléfono que suministra el servicio ADSL y que está ubicada en la pared. Luego, conecte el cable de teléfono desde puerto RJ11 del microfiltro ADSL, que generalmente lleva la etiqueta “DSL”, al puerto RJ11 gris, con la etiqueta “DSL line” en la parte posterior de su router. Conecte todo otro aparato telefónico al otro puerto del microfiltro ADSL, que generalmente lleva la etiqueta “Phone” (teléfono). Se requerirá un microfiltro ADSL adicional para conectar otro dispositivo de telefonía a la misma línea.



Nota: Se incluye un cable para teléfono RJ11. Al insertar un conector RJ11, asegúrese de que la patilla del conector hace clic al introducirlo para asegurarse de que lo ha colocado del modo correcto.

3. Si tiene una línea de teléfono que suministra exclusivamente su servicio ADSL a través de una toma RJ11, simplemente deberá conectar un cable de teléfono desde la toma de la pared al puerto RJ11 gris que lleva la indicación “DSL line”, en la parte posterior de su router.

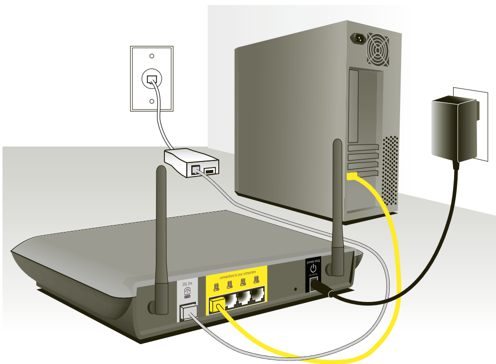
4. Si tiene una toma RJ45 para su servicio ADSL, conecte un convertidor de RJ45 a RJ11 a la toma de la pared. Luego, conecte uno de los extremos del cable de teléfono al convertidor y el otro extremo al puerto RJ11 gris , con la etiqueta “DSL line”, ubicado en la parte posterior de su router.

Nota: En algunos países se suministra el microfiltro ADSL. En otros, no.

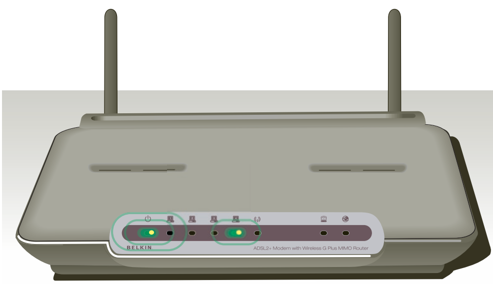
Encendido del router

1. Conecte el adaptador de alimentación suministrado a la entrada del router que indica “Power”.

   Nota: Para una óptima seguridad y rendimiento, utilice únicamente el adaptador de la alimentación incluido. Así, evitará posibles daños al router.



2. Después de conectar el adaptador y de encender la fuente de alimentación, el icono de la alimentación del router...... ubicado en el panel frontal debería encenderse. Puede que el router tarde unos minutos en activarse del todo.



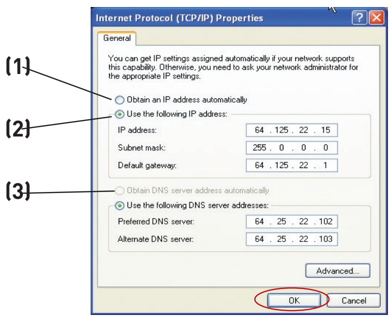
3. Encienda sus ordenadores. Tras arrancar sus ordenadores, el indicador LED de estado LAN...... en la parte frontal del router, se encenderá para cada puerto al que se haya conectado un ordenador mediante cableado. Estas luces indican el estado de conexión y actividad. En este momento está preparado para configurar el router para la conexión ADSL.

Para que su ordenador se pueda comunicar adecuadamente con su router, necesitará cambiar las configuraciones de “TCP/IP / Ethernet” de su PC a “Obtener una dirección IP automáticamente/ Utilizar DHCP”. Esta es la configuración por defecto de la mayoría de los ordenadores domésticos.

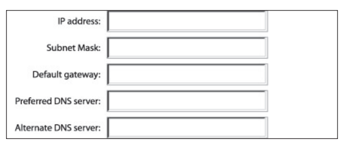
Configure el ordenador que está conectado al módem DSL utilizando PRIMERO los siguientes pasos. Asimismo, puede emplear estos pasos para añadir ordenadores a su router una vez que éste haya sido configurado para conectarse a Internet.

Configuración manual de los adaptadores de red en Windows XP, 2000, o NT

1. Haga clic en “Start” (comienzo), “Settings” (ajustes), y después “Control Panel” (panel de control).
2. Haga doble clic en el icono “Network and dial-up connections” (conexiones telefónicas y de red) (Windows 2000) o en el icono “Network” (red) (Windows XP).
3. Haga clic con el botón derecho del ratón en la “Local Area Connection” (conexión de área local) asociada a su adaptador de red y seleccione “Properties” (propiedades) del menú desplegable.
4. En la ventana “Local Area Connection Properties” (Propiedades de la conexión de área local), haga clic en “Internet” Protocol (TCP/IP)” (Protocolo de Internet [TCP/IP]) y haga clic en el botón “Properties” (Propiedades). Aparecerá la siguiente pantalla:



5. Si se encuentra seleccionada la opción “Use the following IP address” (Utilizar la siguiente dirección IP) **(2)**, su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.

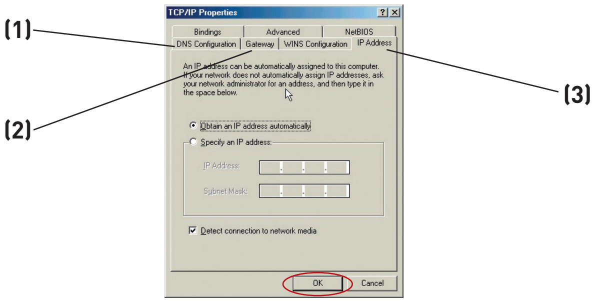


6. Si no se encuentran seleccionadas, seleccione “Obtain an IP address automatically” (obtener una dirección IP automáticamente) **(1)** y “Obtain DNS server address automatically” (obtener una dirección de servidor DNS automáticamente) **(3)**. Haga clic en “OK” (Aceptar).

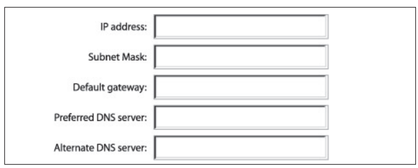
Su(s) adaptador(es) de red está(n) configurado(s) ahora para su uso con el router.

Configuración manual de los adaptadores de red en Windows 98SE o Me

1. Haga clic con el botón derecho del ratón en “My Network Neighborhood” (Mi entorno de red) y seleccione “Properties” (propiedades) del menú desplegable.
2. Seleccione “TCP/IP -> settings” (ajustes TCP/IP) para su adaptador de red instalado. Aparecerá la siguiente ventana.



3. Si se encuentra seleccionada la opción “Specify an IP address” (Especificar una dirección IP), su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.



4. Escriba la dirección IP y la máscara de subred en la pestaña **(3)**.
5. Seleccione la pestaña “Gateway” (Pasarela) **(2)**. Escriba la dirección de gateway (pasarela) en el cuadro.
6. Seleccione la pestaña “DNS Configuration” (Configuración DNS) **(1)**. Escriba la(s) dirección (direcciones) DNS en el cuadro.
7. Si no se encuentra seleccionada, seleccione “Obtain IP address automatically” (Obtener dirección IP automáticamente) en la pestaña de la dirección IP. Haga clic en “OK” (aceptar).
8. Necesitará eliminar la dirección de Gateway (pasarela) de la pestaña de Gateway y las entradas de configuración del Servidor de nombres de dominio para poder configurar la conexión al router de Belkin correctamente.

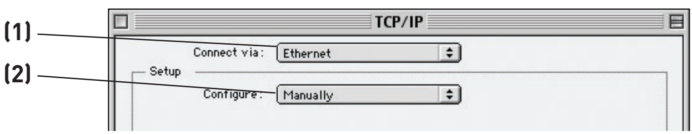
Reinicie el ordenador. Una vez reiniciado el ordenador, el adaptador o los adaptadores de su red estarán configurados ahora para su uso con el router.

Configure el ordenador que está conectado al módem por cable o DSL utilizando PRIMERO los siguientes pasos. Asimismo, puede emplear estos pasos para añadir ordenadores a su Router una vez que éste haya sido configurado para conectar a Internet.

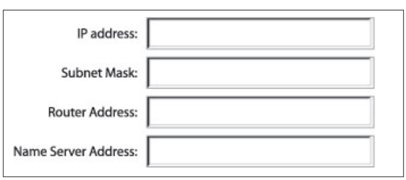
Configuración manual de los ajustes de red en Mac OS hasta 9.x

Para que su ordenador se comunique adecuadamente con su router, necesitará cambiar las configuraciones TCP/IP de su Mac a DHCP.

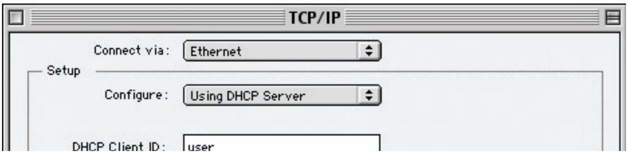
1. Abra el menú Apple. Seleccione “Control Panels” (Paneles de control) y seleccione “TCP/IP”.
2. Aparecerá el panel de control de TCP/IP. Seleccione “Ethernet Built-In” (Ethernet incorporada) o “Ethernet” en el menú desplegable “Connect via:” (conectar a través de:) menú desplegable **(1)**.



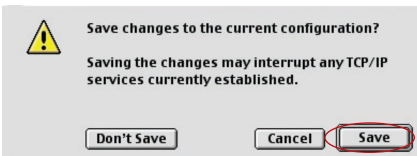
3. Junto a “Configure” (Configurar) **(2)**, si se encuentra seleccionada la opción “Manually” (Manualmente), su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.



4. Si no está establecido todavía, en “Configure:”, (Configurar:) seleccione “Using DHCP Server” (Empleo de servidor DHCP). Esto indicará al ordenador que debe obtener una dirección IP del router.



5. Cierre la ventana. Si ha efectuado algún cambio, aparecerá la siguiente ventana. Haga clic en “Save” (Guardar).



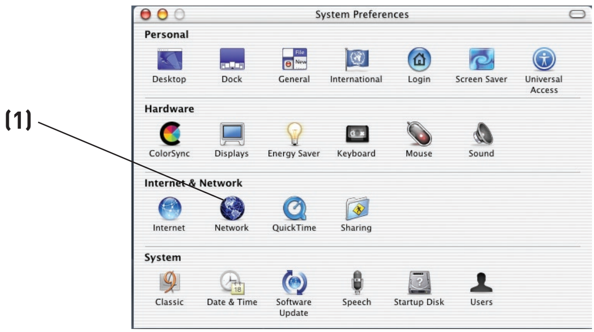
Reinicie el ordenador. Una vez reiniciado el ordenador, los ajustes de su red estarán configurados ahora para su uso con el router.

Configuración manual de los adaptadores de red en Mac OS X

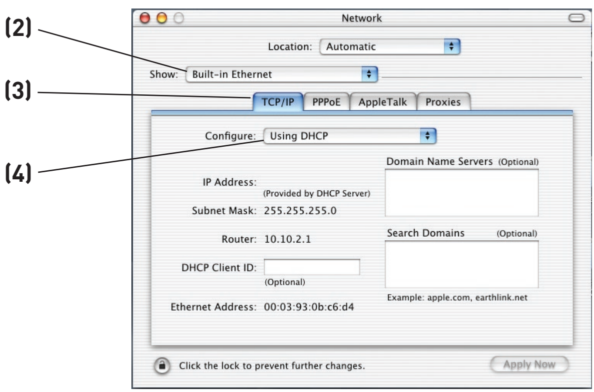
1. Haga clic en el icono de "System Preferences" (Preferencias del sistema).



2. Seleccione "Network" (red) **(1)** del menú "System Preferences" (Preferencias del sistema).

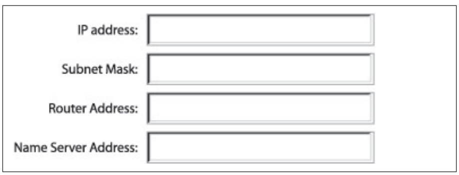


3. Seleccione "Built-in Ethernet" (Ethernet incorporada) **(2)** junto a "Show" (Mostrar) en el menú de red.



4. Seleccione la pestaña “TCP/IP” **(3)**. Junto a “Configure” **(4)**, deberá aparecer “Manually” o “Using DHCP”. En caso contrario, compruebe la pestaña PPPoE **(5)** para asegurarse de que la opción “Connect using PPPoE” (conectar usando PPPoE) NO esté seleccionada. Si está seleccionada, deberá configurar su router para un tipo de conexión PPPoE utilizando su nombre de usuario y contraseña.

5. Si se encuentra seleccionada la opción “Manually” (Manualmente), su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.



6. Si no está establecido todavía, seleccione “Using DHCP Server” (empleo de servidor DHCP).junto a “Configure:” (configurar:) **(4)**, luego haga clic en “Apply Now” (aplicar ahora).

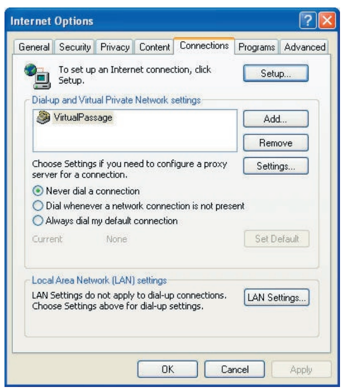
Su(s) adaptador(es) de red está(n) configurado(s) ahora para su uso con el router.

Ajustes recomendados para el navegador de Internet

En la mayoría de los casos, no necesitará efectuar ningún cambio en los ajustes de su navegador de Internet. Si tiene problemas para acceder a Internet o a la interfaz de usuario avanzada a través de Internet, modifique los ajustes de su navegador e introduzca los ajustes recomendados en la presente sección.

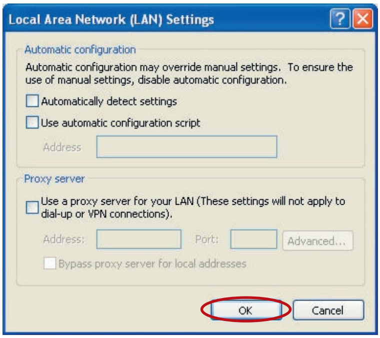


Internet Explorer 4.0 o superior



1. Inicie su navegador de Internet. Seleccione “Tools” (herramientas) y después “Internet Options” (opciones de Internet).
2. En la pantalla de “Internet Options” (opciones de Internet), existen tres posibilidades: “Never dial a connection” (no marcar nunca una conexión), “Dial whenever a network connection is not present” (marcar cuando no haya ninguna conexión a la red) y “Always dial my default connection” (marcar siempre la conexión predeterminada). Si puede elegir una opción, seleccione “Never dial a connection” (no marcar nunca una conexión). Si no puede efectuar una selección, vaya al siguiente paso.
3. En la ventana de “Internet Options” (opciones de Internet), haga clic en “Connections” (conexiones) y seleccione “LAN Settings...” (configuración de LAN).

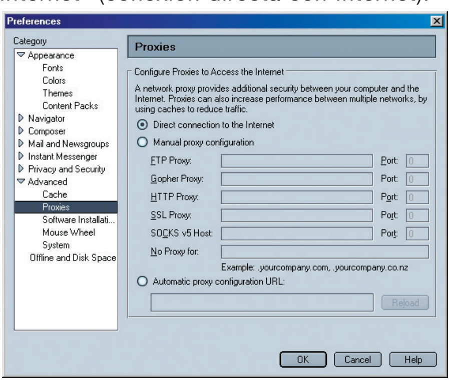
4. Asegúrese de que no existan marcas junto a ninguna de las opciones mostradas: “Automatically detect settings” (detectar la configuración automáticamente), “Use automatic configuration script” (usar secuencia de comandos de configuración automática) y “Use a proxy server” (utilizar un servidor proxy). Haga clic en “OK” (aceptar). Después haga clic de nuevo en “OK” (aceptar) en la página de “Internet Options” (opciones de Internet).



Netscape Navigator 4.0 o superior

1. Inicie Netscape. Haga clic en “Edit” (editar) y seleccione “Preferences” (preferencias).

2. En la ventana de “Preferences” (preferencias), haga clic en “Advanced” (avanzadas) y después seleccione “Proxies” (proxy). En la ventana de “Proxies”, haga clic en “Direct connection to the Internet” (conexión directa con Internet).



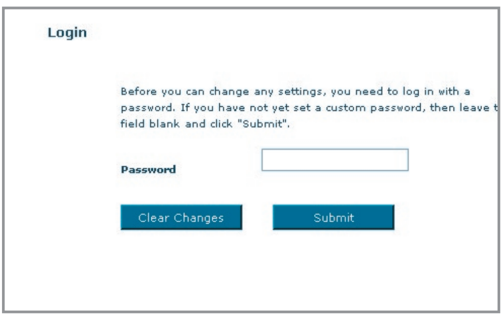
Utilización del asistente de configuración

1. Puede acceder a la interfaz del usuario para la gestión a través de la red del router mediante el navegador de Internet de un ordenador conectado al router. En su navegador, introduzca "192.168.2.1" (no introduzca ningún otro elemento como "http://" o "www"). Después pulse la tecla "Intro".



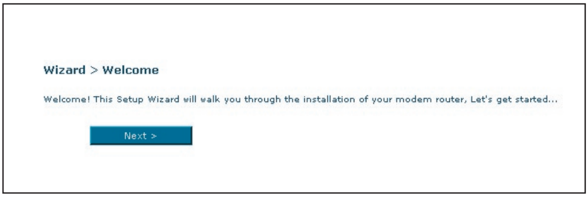
Nota: Para la instalación inicial, se recomienda utilizar un ordenador que esté conectado físicamente al router por medio de un cable RJ45. No se recomienda utilizar un ordenador conectado de manera inalámbrica para la configuración inicial.

2. La siguiente pantalla de acceso aparecerá en el navegador. El router efectúa el envío sin necesidad de introducir contraseña. En la pantalla de acceso, deje la contraseña en blanco y haga clic en el botón "Submit" (enviar) para acceder.

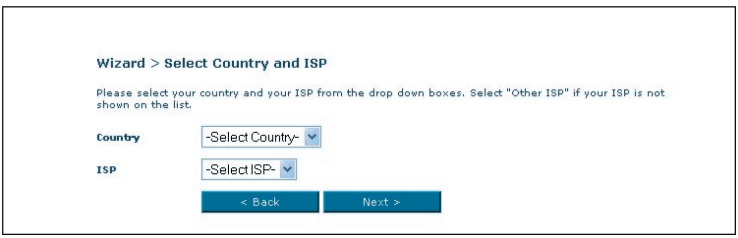


Nota: Se recomienda encarecidamente que modifique la contraseña para su propia seguridad. Lea la siguiente sección, titulada "Configuración manual de su router", para obtener detalles acerca de cómo modificar la contraseña y sobre otros temas respecto a la seguridad.

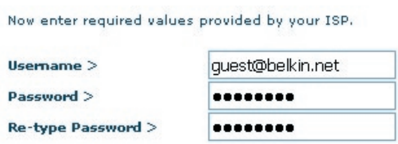
3. El asistente de configuración iniciará automáticamente la instalación rápida (recomendada). Haga clic en “Next” (Siguiente) para continuar.



4 El primer paso es seleccionar su país e ISP, luego haga clic en “Next” (Siguiente). Si su país o ISP no están incluidos en la lista, seleccione “Other Country” (Otro país) u “Other ISP” (Otro ISP).



5 Ahora introduzca el nombre del usuario y contraseña que le ha proporcionado su proveedor de servicios de Internet (ISP) en los campos en blanco. Es importante que introduzca el nombre del usuario y la contraseña correctos. De manera contraria, la conexión fallará. Su ISP podrá confirmar su nombre del usuario y contraseña.



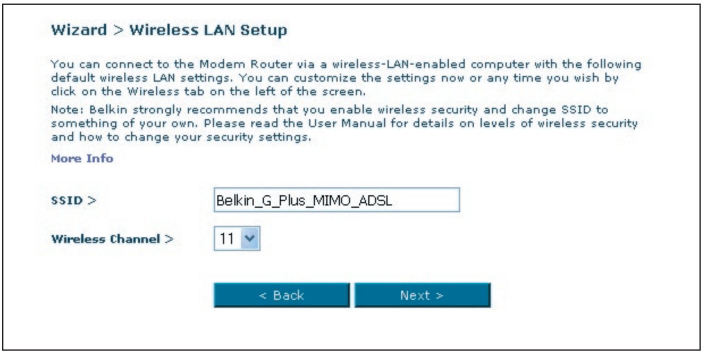
Nota: Para obtener información más detallada acerca de otros tipo de conexiones, consulte la sección “Configuración manual de su router” del presente manual.

6 A continuación aparecerá la ventana de configuración de LAN inalámbrica. Ahora puede conectar el router a través de un ordenador equipado con LAN con las siguientes configuraciones para LAN inalámbrica:

SSID = Belkin G+ MIMO ADSL

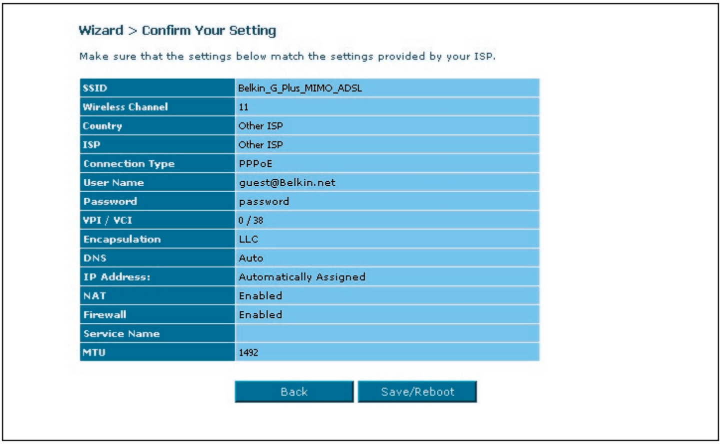
Canal inalámbrico = Auto

Seguridad = desactivada



Nota: Belkin le recomienda encarecidamente que active la seguridad inalámbrica para que funcione con WEP o WPA y que modifique el SSID. Lea el manual del usuario para obtener más información acerca de los niveles de seguridad inalámbrica y de cómo modificar las configuraciones de seguridad.

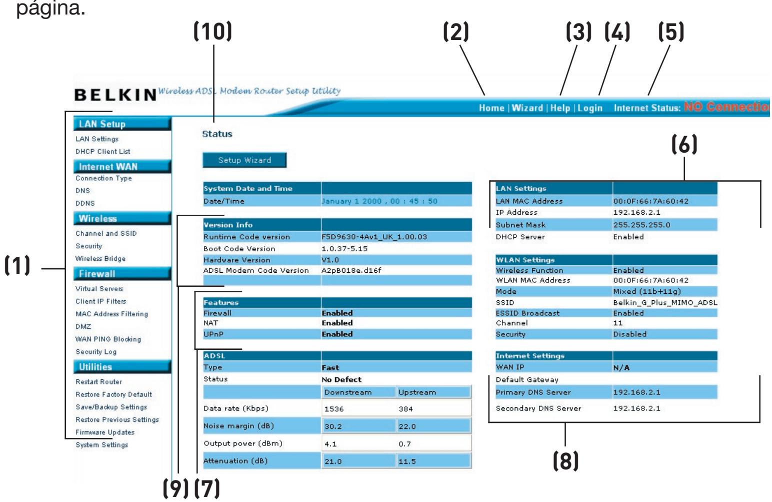
7. Compruebe de nuevo las configuraciones que se muestran en la siguiente pantalla. Haga clic en "Back" (Atrás) para modificar los ajustes o "Apply" (Aceptar) para activar los ajustes.



Nota: Siempre puede reiniciar el asistente de configuración o utilizar el menú de navegación de la izquierda para modificar la configuración.

Utilización de la interfaz de usuario a través de Internet

La página principal le ofrece una imagen rápida del estado y los ajustes del router. Es posible acceder a todas las páginas de configuración avanzada desde esta página.



1. **Vínculos de navegación rápida**
   Puede ir directamente a cualquiera de las páginas de la UI del router haciendo clic directamente en estos vínculos. Los vínculos se encuentran divididos en categorías lógicas y agrupados por pestañas para facilitar la búsqueda de un ajuste concreto. Al hacer clic sobre el encabezamiento de color morado de cada pestaña aparecerá una breve descripción de la función de la misma.
2. **Botón de inicio**
   El botón de Inicio se encuentra disponible en todas las páginas de la UI. Al pulsar este botón, regresará a la página principal o de inicio.
3. **Botón de ayuda**
   El botón de ayuda ("Help") le proporciona el acceso a las páginas de ayuda del router. La opción de ayuda se encuentra disponible asimismo en muchas páginas haciendo clic en la opción "more info" (más información) situada junto a determinadas secciones de cada página.
4. **Botón de "Login"/"Logout" (acceder/salir)**
   Este botón le permite acceder y salir del router pulsando un solo botón. Cuando ha accedido al router, este botón mostrará la palabra "Logout" (salir) El acceso al router le llevará a una página independiente de acceso en la que será preciso introducir una contraseña. Cuando haya accedido al router podrá

efectuar cambios en los ajustes. Cuando haya terminado de realizar los cambios, podrá salir del router haciendo clic sobre el botón de “Logout” (salir). Para obtener más información acerca del acceso al router, consulte la sección “Logging into the Router” (Acceso al router).

5. **Indicador del estado de Internet**

   Este indicador está visible en todas las páginas del router, indicando el estado de la conexión del mismo. Cuando el indicador muestra “connection OK” (Conexión en buen estado) en VERDE, el router se encuentra conectado a Internet. Cuando el router no está conectado a Internet, el indicador en ROJO querrá decir que no hay conexión. El indicador se actualiza automáticamente cuando usted efectúe cambios en las configuraciones del router.

6. **Ajustes LAN**

   Le muestra los ajustes de la parte de la Local Area Network (LAN, red de área local) del router. Es posible efectuar cambios en los ajustes haciendo clic en los vínculos de “Quick Navigation” (Navegación rápida) de la parte izquierda de la pantalla.

7. **Características**

   Le muestra el estado de las funciones NAT, UPnP y firewall del router. Es posible efectuar cambios en los ajustes haciendo clic en cualquiera de los vínculos o haciendo clic en los vínculos de “Quick Navigation” (navegación rápida) de la parte izquierda de la pantalla.

8. **Ajustes de Internet**

Muestra los ajustes de la parte de Internet/WAN del router que se conecta a Internet. Es posible efectuar cambios en cualquiera de estos ajustes haciendo clic en cualquiera de los vínculos o haciendo clic en el vínculo de Navegación rápida “Internet/WAN” de la parte izquierda de la pantalla.

9. **Información sobre la versión**

   Muestra la versión del firmware, la versión del código de arranque, la versión del hardware y el número de serie del router.

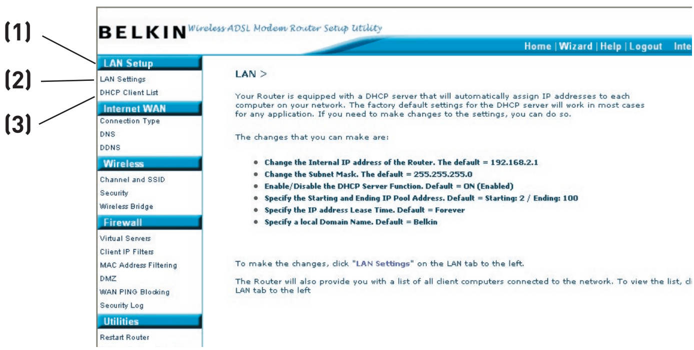
10. **Nombre de la página**

    La página en la que se encuentra puede ser identificada con este nombre. Este manual se referirá en ocasiones a las páginas por el nombre. Por ejemplo, “LAN > LAN Settings se refiere a la página “LAN Settings” (Ajustes LAN).

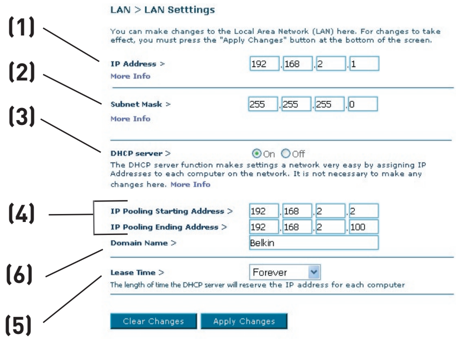
Modificación de los ajustes LAN

Todos los ajustes para la configuración de la LAN interna del router pueden ser visualizados y modificados aquí.

Al hacer clic sobre el encabezamiento de la pestaña LAN **(1)** accederá a la página de encabezamiento de la pestaña LAN. Aquí se puede encontrar una breve descripción de las funciones. Para ver las configuraciones o realizar cambios en alguna de las configuraciones LAN, haga clic sobre “LAN Settings” (Configuraciones LAN) **(2)**, y para ver la lista de ordenadores conectados, haga clic sobre “DHCP client list” (Lista de clientes DHCP) **(3)**.



Ajustes LAN



1. **Dirección IP**

   La “IP address” (dirección IP) es la dirección IP interna del router. La dirección IP predeterminada es “192.168.2.1”. Para acceder a la interfaz de configuración, introduzca esta dirección IP en la barra de direcciones de su navegador. Esta dirección puede ser modificada si es necesario. Para modificar la dirección IP, introduzca la nueva dirección IP y haga clic en “Apply Changes” (Aplicar cambios). La dirección IP que elija debería ser una IP no enrutable. Ejemplos de IP no enrutable son:

   192.168.x.x (donde x es una cifra entre el 0 y el 255)

   10.x.x.x (donde x es una cifra entre el 0 y el 255)

2. **Máscara de subred**

   No es necesario cambiar la máscara de subred ya que el router ajustará automáticamente la longitud según el tipo de dirección IP que tenga.

3. **Servidor DHCP**

   La función de servidor DHCP facilita en gran medida la tarea de establecer una red asignando direcciones IP a cada ordenador de la red de forma automática. El ajuste por defecto es “On” (encendido). El servidor DHCP puede ser APAGADO en caso necesario; sin embargo, para hacerlo deberá establecer de forma manual una dirección IP estática para cada ordenador de su red. Para apagar el servidor DHCP, seleccione “Off” (apagado) y haga clic en “Apply Changes” (aplicar cambios).

4. **Conjunto IP**

   El conjunto de IP es la gama de direcciones IP reservadas para la asignación dinámica a los ordenadores de su red. El valor

predeterminado es 2–100 (99 ordenadores). Si desea modificar este número, puede hacerlo introduciendo una nueva dirección IP de inicio y final y haciendo clic en “Apply Changes” (aplicar cambios). El servidor DHCP puede asignar 100 direcciones IP de forma automática. Esto significa que usted no puede especificar un conjunto de direcciones IP superior a 100 ordenadores. Por ejemplo, si comienza por el 50 deberá finalizar en el 150 o inferior, de forma que no se supere la cifra límite de 100 clientes. La dirección IP de inicio deberá ser inferior en su número a la dirección IP de final.

5. **“Lease Time” (Tiempo límite de concesión)**

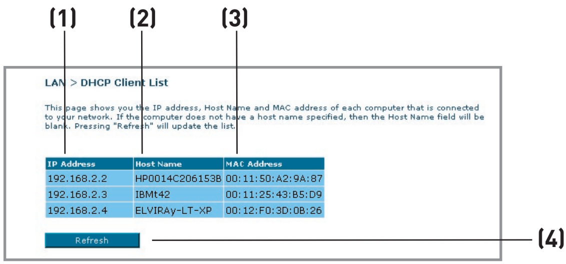
La cantidad de tiempo que el servidor DHCP reservará la dirección IP para cada ordenador. Le recomendamos dejar la configuración del tiempo de mantenimiento en “Forever” (para siempre). El ajuste predeterminado es “Forever” (para siempre), lo que significa que cada vez que el servidor DHCP asigne una dirección IP a un ordenador, la dirección IP no cambiará para ese ordenador concreto. Si configura el tiempo límite de concesión en intervalos menores como un día o una hora, las direcciones IP serán liberadas una vez transcurrido dicho periodo específico de tiempo. Esto significa además que la dirección IP de un ordenador determinado puede cambiar a lo largo del tiempo. Si ha establecido cualquiera otra de las características avanzadas del Router, como DMZ o filtros IP de clientes, éstos dependerán de la dirección IP. Por esta razón, no es deseable para usted que cambie la dirección IP.

6. **Nombre de dominio local**

El ajuste predeterminado es “Belkin”. Puede establecer un nombre de dominio local (nombre de red) para su red. No es necesario modificar esta configuración a no ser que tenga una necesidad avanzada específica para hacerlo. Puede dar a la red el nombre que quiera como “MI RED”.

Lista de clientes DHCP

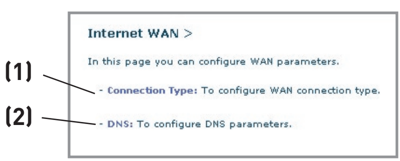
Puede visualizar una lista de los ordenadores (conocidos como clientes) que se encuentran conectados a su red. Puede visualizar la dirección IP **(1)** del ordenador, el nombre de host **(2)** (si se ha asignado uno al ordenador), y la dirección MAC **(3)** de la tarjeta de interfaz de red (NIC, network interface card) del ordenador. Al pulsar el botón "Refresh" (Actualizar) **(4)** se actualizará la lista. Si se han producido cambios, la lista se actualizará.



Internet WAN

La pestaña "Internet/WAN" es donde configurará su router para conectar con su proveedor de servicios de Internet (ISP, Internet Service Provider). El router es capaz de conectarse a prácticamente cualquier sistema de Proveedor de servicios de ADSL siempre que hayan sido configurados correctamente los ajustes del router para su tipo de conexión al ISP. Los ajustes de su conexión le son suministrados por su ISP. Para configurar el router con los ajustes que le ha proporcionado su ISP, haga clic en "Connection Type" (Tipo de conexión) **(1)** en la parte izquierda de la pantalla. Seleccione el tipo de conexión que emplea. Si su ISP le ha proporcionado ajustes DNS, al hacer clic sobre "DNS" **(2)** podrá introducir entradas de direcciones DNS para los ISP que requieran ajustes específicos.

Cuando haya finalizado de realizar los ajustes, el indicador de "Internet Status" (Estado de Internet) mostrará el mensaje "connection OK" (Conexión en buen estado) si su router ha sido configurado correctamente.



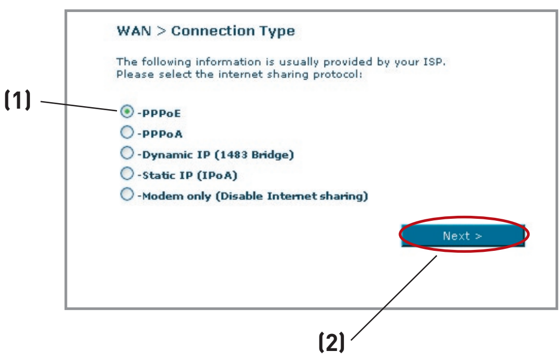
Tipo de conexión

Según los detalles acerca del tipo de conexión que haya obtenido de su ISP, seleccione el tipo de conexión que corresponda:

- PPPoE
- PPPoA
- IP dinámica (1483 Bridged)
- IP estática (IPOA)
- Sólo módem (desactivar compartir Internet)

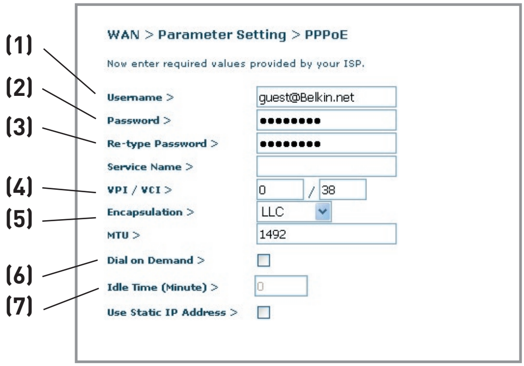
Nota: En el anexo C de este manual del usuario encontrará algunos de los parámetros más frecuentes para Internet DSL. Si tiene dudas, consulte a su ISP.

Seleccione el tipo de conexión que emplea haciendo clic en el botón **(1)** situado junto a su tipo de conexión y después haciendo clic en "Next" (Siguiente) **(2)**.



Establecimiento del tipo de conexión de su ISP como PPPoE o PPPoA

PPPoE (Protocolo punto a punto a través de Ethernet) es el método estándar de conexión de dispositivos de red. Requiere un nombre de usuario y una contraseña para acceder a la red de su ISP y conectarse a Internet. PPPoA (PPP sobre ATM) es similar a PPPoE. Es muy frecuente en el Reino Unido. Seleccione PPPoE o PPPoA y haga clic en “Next” (Siguiente). Luego, introduzca la información que le ha proporcionado su ISP y haga clic en “Apply Changes” (Aplicar cambios) para activar los ajuste



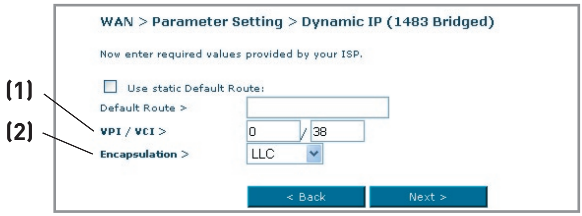
1. **Nombre de usuario -** Introduzca el nombre de usuario. (Suministrado por su ISP).
2. **Contraseña -** Introduzca su contraseña. (Suministrado por su ISP).
3. **Confirmación de la contraseña -** Vuelva a introducir la contraseña. (Suministrado por su ISP).
4. **VPI/VCI -** Introduzca aquí los parámetros de su identificador de ruta virtual (VPI) y del identificador de circuito virtual (VCI). (Suministrado por su ISP).
5. **Encapsulamiento -** Seleccione el tipo de encapsulamiento correspondiente (suministrado por su ISP) para especificar cómo manejar múltiples protocolos en la capa de transporte ATM.

   VC-MUX: PPPoA Circuito Virtual Multiplexeado (encapsulamiento anulado) permite sólo un protocolo por circuito virtual con poca sobrecarga.

   LLC: PPPoA Control de Enlace Lógico permite múltiples protocolos sobre un único circuito virtual (con más sobrecarga).
6. **Conexión telefónica por demanda -** - Al seleccionar “Dial on Demand” (Conexión telefónica por demanda), su router se conectará automáticamente a Internet cuando un usuario abra el navegador de Internet.
7. **Idle Time (tiempo límite de inactividad) -** Introduzca aquí el tiempo límite de inactividad (en minutos) para la conexión a Internet. Cuando haya transcurrido este período de tiempo, la conexión finalizará.

Establecimiento del tipo de conexión como IP dinámica (1483 Bridged)

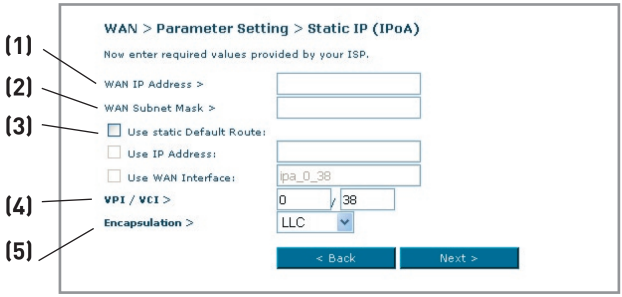
Este método de conexión crea un puente entre su red y la de su ISP. El router obtendrá automáticamente una dirección de IP del servidor DHCP de su ISP.



1. **VPI/VCI -** Introduzca aquí los parámetros de su identificador de ruta virtual (VPI) y del identificador de circuito virtual (VCI). Estos identificadores le serán suministrados por su ISP.
2. **Encapsulamiento -** Seleccione LLC o VC MUX que utiliza su ISP.

Establecimiento de su tipo de conexión al ISP como IP estático (IPoA)

Este tipo de conexión también se denomina “Clásico IP sobre ATM” o “CLIP”, en el cual su ISP le proporciona un IP fijo para que su router se conecte al Internet.

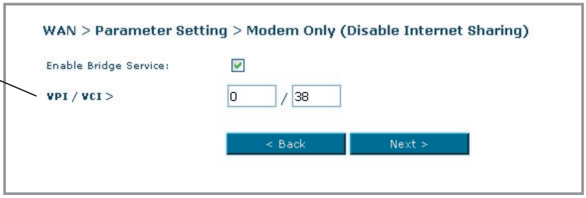


1. **WAN IP Address –** Introduzca la dirección de IP que le ha asignado su ISP para la interfaz WAN de su router.
2. **Máscara de subred WAN -** Introduzca la máscara de subred que le ha asignado su ISP.
3. **Ruta por defecto -** Introduzca una dirección IP de gateway por defecto. Si el router no puede encontrar la dirección de destino dentro de la red local, reenviará los paquetes a la pasarela por defecto que le ha asignado su ISP.
4. **VPI/VCI -** Introduzca aquí los parámetros de su identificador de ruta virtual (VPI) y del identificador de circuito virtual (VCI). Estos identificadores le serán suministrados por su ISP.
5. **Encapsulamiento -** Seleccione LLC o VC MUX que utiliza su ISP.

Establecimiento del tipo de conexión como "Sólo módem" (desactivar compartir Internet)

En este modo, el router actúa sólo como puente por el que pasan los paquetes hacia el puerto DSL. Requiere la instalación de software adicional que debe ser instalado en su ordenador para poder acceder a Internet.

(1)

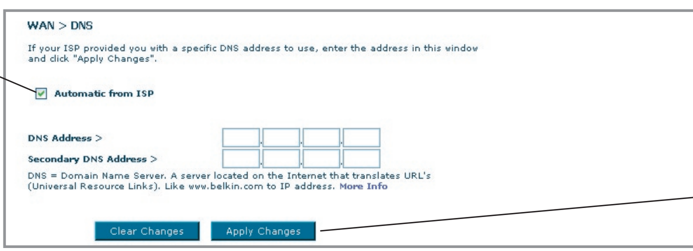


1. **VPI/VCI -** Introduzca aquí los parámetros de su identificador de ruta virtual (VPI) y del identificador de circuito virtual (VCI). (Suministrado por su ISP).

Ajustes de DNS (Servidor de nombres de dominio)

Un "Domain Name Server" es un servidor ubicado en Internet que convierte los Universal Resource Locater (URL, Localizador de recursos universales) como "www.belkin.com" en direcciones IP. Muchos ISP no precisan que usted introduzca esta información en el router. El recuadro "Automatic from ISP" (automáticamente desde el ISP)**(1)** deberá encontrarse marcado si su ISP no la ha proporcionado ninguna dirección DNS específica. Si está utilizando un tipo de conexión de IP estática, es posible que deba introducir una dirección DNS específica y una dirección DNS secundaria para que su conexión funcione correctamente. Si su tipo de conexión es dinámica o PPPoE, es probable que no sea necesario introducir ninguna dirección DNS. Deje marcado el recuadro "Automatic from ISP" (Automáticamente desde el ISP). Para introducir los ajustes de la dirección DNS, retire la marca del recuadro "Automatic from ISP" (Automáticamente desde el ISP) e introduzca sus entradas DNS en los espacios previstos. Haga clic en "Apply Changes" (Aplicar cambios) **(2)** para guardar los ajustes.

(1)



(2)

Uso de DNS dinámico

El servicio DNS dinámico le permite otorgar a una dirección IP dinámica uno de los muchos nombres de host estático que ofrece la lista de dominios de DynDNS.org; de esta manera, podrá acceder a sus ordenadores en red de manera más sencilla desde varias ubicaciones en Internet. DynDNS.org ofrece a la comunidad de Internet este servicio para hasta cinco nombres de host en forma gratuita.

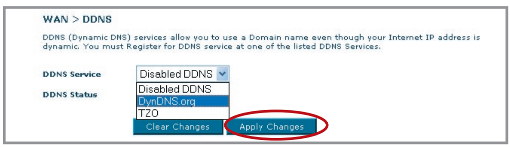
El servicio DNSSM dinámico es ideal para una página web personal, un servidor de archivos o para facilitar el acceso a su PC del hogar y los archivos guardados cuando está en el trabajo. Mediante la utilización de este servicio puede estar seguro de que el nombre de host siempre indicará a su dirección IP, independientemente de cuántas veces su ISP la cambie. Cuando su dirección IP cambia, sus amigos y socios pueden ubicarlo siempre visitando sunombre.dyndns.org.

Puede registrarse de manera gratuita para obtener su nombre de host DNS dinámico en http://www.dyndns.org.

Configuración del cliente de actualización para DNS dinámico del router

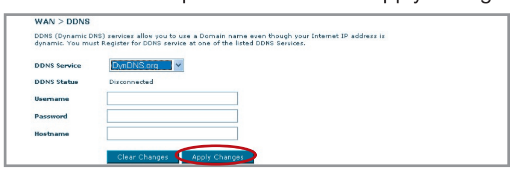
Debe registrarse para el servicio gratuito de actualización de DynDNS.org antes de poder utilizar esta función. Una vez que se haya registrado, siga las instrucciones a continuación.

1. Seleccione "DynDNS.org" del cuadro desplegable. Haga clic sobre "Apply Changes" (aplicar cambios)



2. ntroduzca su nombre de usuario de DynDNS.org en el campo "User Name" (nombre de usuario)**(1)**.
3. Introduzca la palabra clave de DynDNS.org en el campo "Password" (contraseña) **(2)**.
4. Introduzca el nombre de dominio de DynDNS.org que ha configurado en DynDNS.org en el campo "Domain name" (Nombre de dominio) **(3)**.
5. Haga clic en "Apply Changes" (aplicar cambios) para actualizar la dirección IP.

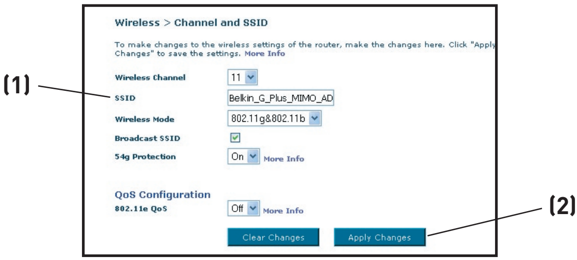
Si la dirección IP dinámica que le ha asignado su ISP cambia, el router actualizará automáticamente los servidores de DynDNS.org con la dirección IP nueva. También puede hacer esto de manera manual pulsando el botón "Apply Changes" (Aplicar cambios) **(4)**.



Inalámbrico

La pestaña “Wireless” (Inalámbrico) le permite realizar cambios en los ajustes de red inalámbrica. Desde esta pestaña puede efectuar cambios en el nombre de red inalámbrica (SSID), el canal de funcionamiento y en los ajustes de seguridad en la encriptación.

Canal y SSID



1. Modificación del canal inalámbrico

Existe una serie de canales de funcionamiento entre los que puede elegir. En Estados Unidos, existen 11 canales. En el Reino Unido y la mayor parte de Europa, existen 13 canales. Un pequeño número de países presenta otros requisitos respecto a los canales. Su router está configurado para funcionar en los canales apropiados para el país en que reside. El canal por defecto es el 11 (a menos que se encuentre en un país que no permita el canal 11). Este canal puede ser modificado en caso necesario. Si existen otras redes inalámbricas operando en su área, su red deberá ser configurada para funcionar en un canal diferente que el resto de las redes inalámbricas. Para lograr un mejor rendimiento, utilice un canal que se encuentre al menos a cinco canales de distancia del de las otras redes inalámbricas. Por ejemplo, si la otra red está funcionando en el canal 11, configure su red en el canal 6 o en un canal inferior. Para modificar el canal, selecciónelo de la lista desplegable. Haga clic sobre “Apply Changes” (Aplicar cambios). La modificación es inmediata.

2. Modificación del Nombre de red inalámbrica (SSID)

Para identificar su red inalámbrica, se emplea un nombre conocido como SSID (Service Set Identifier, Identificador del conjunto de servicios). El SSID por defecto del router es “belkin54g”. Puede cambiar este nombre por el que desee o puede dejarlo sin modificar. Si existen otras redes inalámbricas operando en su área, deberá asegurarse de que que su SSID sea exclusivo (no coincida con el de otra red inalámbrica en la zona). Para modificar el SSID, introduzca en el campo SSID **(1)** el SSID que desee y haga clic en “Apply Changes” (Aplicar cambios) **(2)**. La modificación es inmediata. Si modifica el SSID, es posible que sus ordenadores

de equipamiento inalámbrico deban ser configurados de nuevo con su nuevo nombre de red. Consulte la documentación de su adaptador de red inalámbrica para obtener información acerca de cómo realizar esta modificación.

3. Utilización de la función de ESSID Broadcast

Para garantizar la seguridad máxima, deberá optar por no emitir el SSID de su red. Al hacerlo así, mantendrá su nombre de red oculto a los ordenadores que estén rastreando la presencia de redes inalámbricas. Para desactivar la emisión de SSID, retire la marca del recuadro situado junto a “Broadcast SSID” (Emitir SSID). La modificación es inmediata. Ahora será preciso configurar cada ordenador para conectar con su SSID específico; ya no se aceptará la opción “ANY” (Cualquiera) para el SSID. Consulte la documentación de su adaptador de red inalámbrica para obtener información acerca de cómo realizar esta modificación.

Nota: Esta característica avanzada deberá ser empleada exclusivamente por usuarios avanzados.

4. Utilización del conmutador del modo inalámbrico

Su router puede funcionar en dos modos inalámbricos diferentes:

- **802.11b & 802.11g-** Elija esta opción si planea tener clientes inalámbricos de 802.11b y 802.11g conectados a su red.
- **802.11g -** Utiliza esta opción si no existen clientes 802.11b en la red. Esta opción ofrece las mejores prestaciones, pero no permitirá conectarse a los clientes 802.11b.

5. Conmutador de modo protegido

Como parte de la especificación 802.11g, el Modo Protegido garantiza el funcionamiento correcto de los clientes 802.11g y de los puntos de acceso cuando existe un tráfico 802.11b intenso en el entorno de actividad. Cuando el modo Protegido está ENCENDIDO, el 802.11g busca otro tráfico de red inalámbrica antes de transmitir los datos. Por lo tanto, la utilización de este modo en entornos con tráfico 802.11b INTENSO o con interferencia produce los mejores resultados en cuanto a rendimiento. Si se encuentra en un entorno en el que existe un tráfico reducido—o no existe ningún tráfico—de red inalámbrica, se logrará el mejor rendimiento si el modo Protegido se encuentra APAGADO.

Encriptación/seguridad:

Cómo proteger su red Wi-Fi

Presentamos diferentes formas de potenciar la seguridad de su red inalámbrica y de proteger sus datos de intrusiones no deseadas. Esta sección está destinada al usuario de una pequeña oficina, oficina en el hogar y del hogar. Al momento de la publicación de este manual, se encuentran disponibles tres métodos de encriptación.

Nombre	Privacidad equivalente a la del cable de 64 bits	Privacidad equivalente a la del cable de 128 bits	Acceso protegido Wi-Fi - TKIP	Acceso Protegido Wi-Fi 2
Acrónimo	WEP de 64 bits	WEP de 128 bits	WPA-TKIP/AES (o solamente WPA)	WPA2-AES (o solamente WPA2)
Seguridad	Bueno	Mejor	El mejor	El mejor
Característi-cas	Claves estáti-cas	Claves estáticas	Encriptación de clave dinámica y autenticación mutua	Encriptación de clave dinámica y autenticación mutua
	Claves de encriptación basadas en el algoritmo RC4 (habitualmente claves de 40 bits)	Mayor seguridad que la WEP de 64 bits empleando una longitud de clave de 104 bits, más 24 bits adicionales de datos generados por el sistema	TKIP (protocolo de integridad de clave temporal) adicional para permitir la rotación de las claves y el fortalecimiento de la encriptación	El AES (Advanced Encryption Standard, estándar de encriptación avanzada) no causa ninguna pérdida de rendimiento

WEP (Wired Equivalent Privacy, Privacidad equivalente a la del cable)

La WEP (Wired Equivalent Privacy, privacidad equivalente a la del cable) es un protocolo común que añade seguridad a todos los productos inalámbricos compatibles con Wi-Fi. La WEP ha sido diseñada para aportar a las redes inalámbricas un nivel de protección de la privacidad equivalente al de una red por cable.

WEP de 64 bits

La WEP de 64 bits se introdujo en un principio con encriptación de 64 bits, que incluye una longitud de clave de 40 bits más 24 bits adicionales

de datos generados por el sistema (64 bits en total). Algunos fabricantes de hardware llaman encriptación de 40 bits a la encriptación de 64 bits. Poco después de que se introdujese esta tecnología, los investigadores descubrieron que la encriptación de 64 bits era demasiado fácil de descodificar.

WEP de 128 bits

Como resultado de una debilidad potencial en la seguridad WEP de 64 bits, se creó el método de encriptación de 128 bits que ofrece un nivel de seguridad más alto. La encriptación de 128 bits incluye una longitud de clave de 104 bits, más 24 bits adicionales de datos generados por el sistema (128 bits en total). Algunos fabricantes de hardware llaman encriptación de 104 bits a la encriptación de 128 bits.

La mayoría de equipos inalámbricos actualmente en el mercado son compatibles con la encriptación WEP tanto de 64 bits como de 128 bits, pero es posible que usted disponga de equipos más antiguos que sólo sean compatibles con la encriptación WEP de 64 bits. Todos los productos inalámbricos de Belkin son válidos para la WEP de 64 bits y de 128 bits.

Claves de encriptación

Después de seleccionar el modo de encriptación WEP de 64 bits o de 128 bits, es esencial generar una clave de encriptación. Si la clave de encriptación no es igual para el conjunto de la red inalámbrica, sus dispositivos de interconexión en red inalámbrica no podrán comunicarse entre sí dentro de su red y usted no podrá comunicarse con éxito dentro de la misma.

Puede introducir su clave hexadecimal de forma manual, o introducir una frase de paso en el campo “Passphrase” (frase de paso) y hacer clic en “Generate” (generar) para crear una clave. Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9. Para WEP de 64 bits deberá introducir 10 claves hexadecimales. Para la WEP de 128 bits, deberá introducir 26 claves hexadecimales.

La frase de paso WEP NO es lo mismo que la clave WEP. Su tarjeta inalámbrica utiliza esta contraseña para generar sus claves WEP, pero es posible que los diferentes fabricantes de hardware dispongan de diferentes métodos para generar las claves. Si cuenta en su red con equipos de diferentes vendedores, lo más sencillo será utilizar la clave WEP hexadecimal de su router o punto de acceso e introducirla manualmente en la tabla de claves WEP hexadecimales de la pantalla de configuración de su tarjeta.

Cómo utilizar una clave hexadecimal

Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9. Las claves de 64 bits son cinco cifras de dos dígitos. Las claves de 128 bits son 13 cifras de dos dígitos.

Por ejemplo:
AF 0F 4B C3 D4 = clave de 64 bits
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clave de 128 bits
En las siguientes casillas, invente su clave escribiendo dos caracteres entre A–F y 0–9 en cada casilla. Empleará esta clave para programar los ajustes de encriptación de su router y sus ordenadores inalámbricos.

Nota para los usuarios de Mac: Los productos originales Apple AirPort® admiten exclusivamente la encriptación de 64 bits. Los productos Apple AirPort 2 admiten la encriptación de 64 o de 128 bits. Compruebe qué versión del producto está utilizando. Si no puede configurar su red con una encriptación de 128 bits, pruebe con una encriptación de 64 bits.

WPA (acceso protegido Wi-Fi)

El WPA (Wi-Fi Protected Access, Acceso Wi-Fi protegido) es un nuevo estándar Wi-Fi diseñado para mejorar las propiedades de seguridad de la WEP. Para utilizar la seguridad WPA, los controladores y el software de su equipo inalámbrico deben actualizarse para que sean compatibles con el WPA. Estas actualizaciones se encontrarán en la página web del vendedor de su equipo inalámbrico. Existen dos tipos de seguridad WPA: WPA-Personal (PSK) y WPA-Enterprise (RADIUS).

WPA-Personal (PSK)

Este método emplea como clave de red lo que se conoce como “clave precompartida”. Una clave de red es una frase de acceso que contiene entre ocho y 63 caracteres de largo. Se compone de una combinación de letras, números o caracteres. Todos los clientes emplean la misma clave para acceder a la red. Normalmente, este es el modo que se utilizará en un entorno doméstico.

WPA-Enterprise (RADIUS)

Con este sistema, un servidor Radius distribuye la clave de red automáticamente a los clientes. Está vinculado habitualmente a un entorno empresarial. Para obtener una lista de los productos inalámbricos de Belkin que son compatibles con WPA, visite nuestro sitio web **www.belkin.com/networking**.

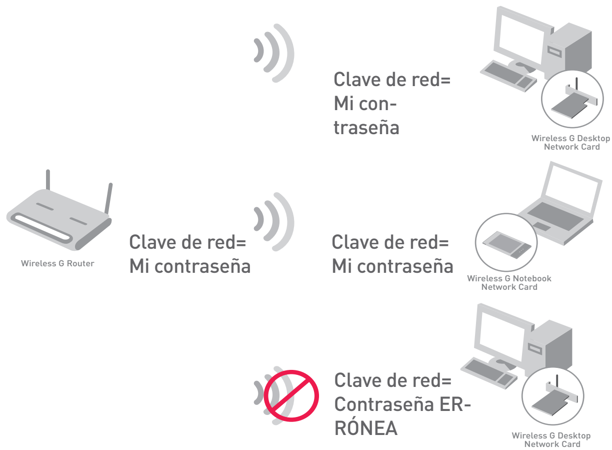
WPA2 (WiFi Protected Access)

WPA2 es la segunda generación del estándar 802.11i basado en WPA. Ofrece un nivel más alto de seguridad inalámbrico ya que combina una autenticación de red avanzada con un método de encriptación AES más fuerte. Al igual que la seguridad WPA, WPA2 está disponible tanto en modo WPA2-Personal (PSK) como en modo Enterprise (RADIUS). Normalmente, WPA2-Personal (PSK) es el modo que se utiliza en los entornos para casa, mientras que WPA2-Enterprise (RADIUS) se emplea en los entornos profesionales donde un servidor radius externo distribuye la clave de la red a los clientes de forma automática.

Compartir las mismas claves de red

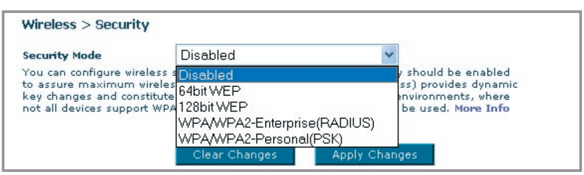
La mayoría de productos Wi-Fi se suministran con la seguridad desconectada. Por esta razón, una vez que haya puesto en funcionamiento su red, deberá activar las opciones de seguridad WEP, WPA o WPA2 y asegurarse de que todos sus dispositivos de red inalámbrica compartan la misma clave de red.

La tarjeta de red inalámbrica G + MIMO para ordenador de sobremesa no puede acceder a la red porque emplea una clave de red diferente de la configurada en el router inalámbrico G + MIMO.



Modificación de los ajustes de encriptación inalámbrica

Su router está equipado con WPA/WPA2 (Wireless Protected Access, Acceso Inalámbrico Protegido), el estándar de seguridad inalámbrica más moderno. También es compatible con el estándar anterior de seguridad llamado WEP (Privacidad Equivalente Cableada). De forma predeterminada, la seguridad inalámbrica está desactivada. Para activar la seguridad, primero deberá determinar qué estándar desea utilizar. Para acceder a los ajustes de seguridad, haga clic **en "Security" (Seguridad) en la pestaña "Wireless " (Inalámbrico).**



Configuración WEP

Encriptación WEP de 64 bits

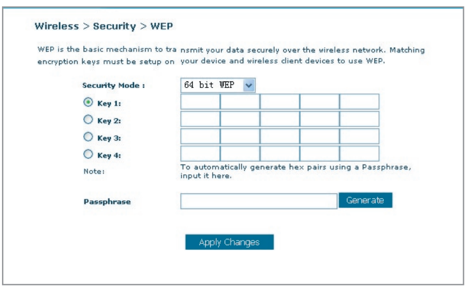
1. Seleccione “64-bit WEP” (WEP de 64 bits) del menú desplegable.

2. Después de seleccionar su modo de encriptación WEP, podrá introducir su clave tecleando la clave hexadecimal manualmente.

Una clave hexadecimal es una combinación de números y letras de la A a la F y del 0 al 9. Para WEP de 64 bits deberá introducir 10 claves hexadecimales.

Por ejemplo:

AF 0F 4B C3 D4 = clave WEP de 64 bits



3. Haga clic en “Apply Changes” (Aplicar cambios) para finalizar. Ahora está establecida la encriptación en el router. Cada ordenador de su red inalámbrica deberá ser configurado ahora con los mismos ajustes de seguridad..

ATENCIÓN: Si está configurando el router inalámbrico o punto de acceso desde un ordenador con un cliente inalámbrico, perderá la conexión hasta que haya activado la función de seguridad de su cliente inalámbrico. Asegúrese de anotar la clave antes de aplicar los cambios.

Encriptación WEP de 128 bits

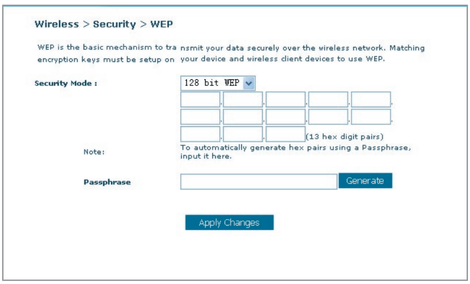
1. Seleccione "128-bit WEP" (WEP de 64 bits) del menú desplegable.

2. Después de seleccionar su modo de encriptación WEP, podrá introducir su clave tecleando la clave hexadecimal manualmente.

   Una clave hexadecimal es una combinación de números y letras de la A a la F y del 0 al 9. Para WEP de 128 bits deberá introducir 26 claves hexadecimales.

   Por ejemplo:

   C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clave WEP de 128-bits



3. Haga clic en "Apply Changes" (Aplicar cambios) para finalizar. Ahora está establecida la encriptación en el router. Cada ordenador de su red inalámbrica deberá ser configurado ahora con los mismos ajustes de seguridad..

ATENCIÓN: Si está configurando el router inalámbrico o punto de acceso desde un ordenador con un cliente inalámbrico, perderá la conexión hasta que haya activado la función de seguridad de su cliente inalámbrico. Asegúrese de anotar la clave antes de aplicar los cambios.

Configuración WPA

Nota: Para utilizar la seguridad WPA, todos sus clientes deberán haber actualizado los controladores y el software compatibles. Al momento de la publicación de este manual, se puede descargar de Microsoft un parche de seguridad gratuito. Este parche sólo funciona con el sistema operativo Windows XP. Asimismo, deberá descargar el driver más actualizado para su tarjeta de red inalámbrica G para ordenador de sobremesa o para

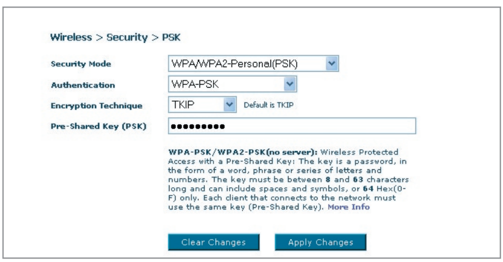
notebook de Belkin desde la página de servicio de atención al cliente de Belkin. En la actualidad no existe soporte para otros sistemas operativos. El parche de Microsoft sólo es compatible con dispositivos con controladores preparados para WPA, como los productos 802.11g de Belkin.

Existen dos tipos de seguridad WPA: WPA-Personal (PSK) y WPA-Enterprise (RADIUS). WPA-Personal (PSK) emplea como clave de seguridad lo que se conoce como una “clave precompartida”. Una clave precompartida es una contraseña de entre ocho y 63 caracteres de largo. Se compone de cualquier combinación de letras, números y otros caracteres. Todos los clientes emplean la misma clave para acceder a la red. Normalmente, este modo se utilizará en un entorno doméstico.

WPA-Enterprise (RADIUS) es una configuración en la que un servidor Radius distribuye las claves a los clientes de forma automática. Se emplea habitualmente en un entorno empresarial.

Cómo establecer una WPA-Personal (PSK)

1. Desde el menú desplegable del modo de seguridad “Security Mode”, seleccione “WPA/WPA2-PSK.
2. Seleccione “WPA-PSK” para la autenticación.
3. Para la técnica de encriptación “Encryption Technique”, seleccione “TKIP”. Este ajuste deberá ser idéntico en todos los clientes que instale.
4. Introduzca su clave precompartida. Puede estar compuesta por entre ocho y 63 caracteres entre letras, números y símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale. Por ejemplo, su PSK será algo así como: “Clave de red familia Pérez”.



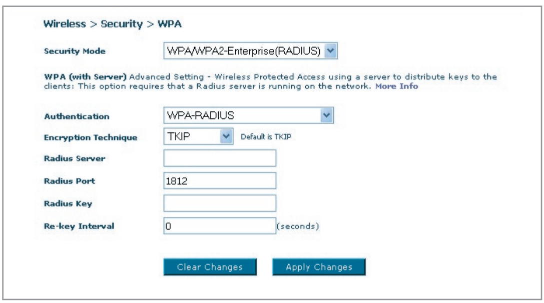
5. Haga clic en “Apply Changes” (Aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Establecer ajustes para WPA-Enterprise (RADIUS)

Si su red emplea un servidor Radius para distribuir las claves a los clientes, utilice este ajuste.

1. Desde el menú desplegable del modo de seguridad “Security Mode”, seleccione “WPA/WPA2—Enterprise (RADIUS)

2. Seleccione “WPA-RADIUS” para la autenticación
3. Para la técnica de encriptación “Encryption Technique”, seleccione “TKIP”. Este ajuste deberá ser idéntico en los clientes que instale.
4. Introduzca la dirección IP del servidor Radius en los campos de “Radius
Server”.
5. Introduzca la clave Radius en el campo “Radius Key”.
6. Introduzca el intervalo de la clave. El intervalo de clave es la frecuencia con la que se distribuyen las claves (en paquetes).
7. Haga clic en “Apply Changes” (Aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.



Requisitos para WPA2

IMPORTANTE: Para utilizar la seguridad WPA2, todos sus ordenadores y adaptadores de clientes inalámbricos deberán haber actualizado los parches, controladores y software que son compatibles con WPA2. Al momento de la publicación de este manual, se puede descargar de Microsoft una serie de parches de seguridad gratuitos. Estos parches sólo funcionan con el sistema operativo Windows XP. En la actualidad no existe soporte para otros sistemas operativos.

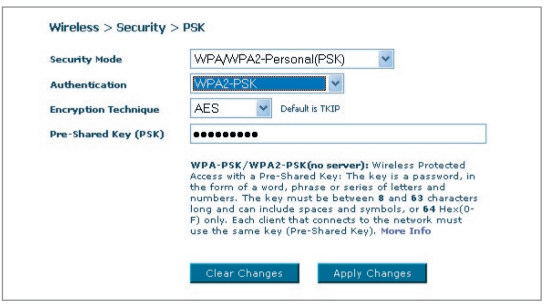
Para ordenadores con Windows XP que no tengan el Service Pack 2 (SP2), puede descargar un archivo de Microsoft llamado “Windows XP Support Patch for Wireless Protected Access (KB 826942)” que está disponible en: http://support.microsoft.com/?kbid=826942

Para Windows XP con Service Pack 2, Microsoft ofrece una descarga gratuita para actualizar los clientes inalámbricos de modo que éstos puedan admitir WPA2 (KB893357). Puede descargar la actualización de: http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

IMPORTANTE: Debe también asegurarse de que todas las tarjetas o adaptadores inalámbricos de los clientes admitan WPA2 y de haber descargado e instalado el controlador más reciente. La mayoría de las tarjetas inalámbricas de Belkin tienen un driver actualizado que puede ser descargado de la página de soporte de Belkin: www.belkin.com/networking.

Cómo establecer una WPA2-Personal (PSK)

1. Desde el menú desplegable “Security mode” (modo de seguridad), seleccione “WPA/WPA2-PSK (PSK)”.
2. Seleccione “WPA2-Personal (PSK)” para la autenticación.
3. Para la técnica de encriptación (“Encryption Technique”), seleccione “AES”. Este ajuste deberá ser idéntico en todos los clientes que instale.
4. Introduzca su clave precompartida. Puede estar compuesta por entre ocho y 63 caracteres entre letras, números y símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale. Por ejemplo, su PSK será algo así como: “Clave de red familia Pérez”.



5. Haga clic en “Apply Changes” (aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

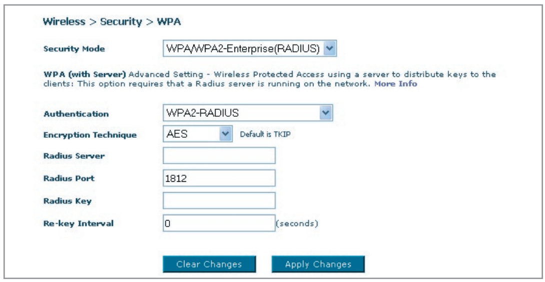
Establecer ajustes para WPA2-Enterprise (RADIUS)

Si su red emplea un servidor Radius para distribuir las claves a los clientes,

utilice este ajuste.

1. FDesde el menú desplegable “Security mode” (modo de seguridad), seleccione “WPA/WPA2—Enterprise (RADIUS)”.

2. Seleccione “WPA2-RADIUS” para la autenticación
3. Para la técnica de encriptación (“Encryption Technique”), seleccione “AES”. Este ajuste deberá ser idéntico en los clientes que instale.
4. Introduzca la dirección IP del servidor Radius en los campos de “Radius Server”.
5. Introduzca la clave Radius en el campo “Radius Key”.
6. Introduzca el intervalo de la clave. El intervalo de clave es la frecuencia con la que se distribuyen las claves (en paquetes).
7. Haga clic en “Apply Changes” (aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.



IMPORTANTE:
Asegúrese de actualizar sus ordenadores inalámbricos con el modo WPA2 y de haber establecido los ajustes correctos para poder establecer una conexión adecuada con el router.

Configure el adaptaor de red de su ordenador para utilizar la seguridad

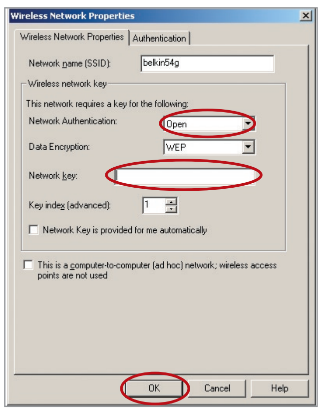
Atención: Esta sección le proporcionará información acerca de cómo configurar los adaptadores de red de sus ordenadores para emplear seguridad. En este momento, ya debe tener su router inalámbrico o punto de acceso configurado para utilizar WPA2, WPA o WEP. Para obtener una conexión inalámbrica, necesitará configurar su tarjeta inalámbrica para ordenador portátil y su tarjeta inalámbrica para ordenador de sobremesa de tal manera que utilicen las mismas configuraciones de seguridad.

Las Tarjetas de red G+ MIMO de Belkin disponen de una utilidad de red inalámbrica fácil de usar. Simplemente haga clic en el nombre de su red inalámbrica (SSID) de la lista de redes disponibles, e introduzca su clave precompartida. Para más información, consulte el manual de usuario de la Tarjeta para red de Belkin.

La mayoría de los ordenadores también pueden configurarse para funcionar con la pantalla de Redes inalámbricas: propiedades que incluye el sistema operativo Microsoft Windows. A continuación se presentan dos ejemplos:

Conexión de su ordenador a una red inalámbrica que requiera una clave WEP de 64 bits o de 128 bits:

1. Haga doble clic sobre este icono de “Indicador de señal” para abrir la pantalla “Wireless Network” (Utilidad de red inalámbrica). El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta inalámbrica.
2. En la pestaña “Wireless Network Properties” (Redes inalámbricas: propiedades), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
3. En la categoría “Data Encryption” (Encriptación de datos), seleccione “WEP”.
4. Asegúrese de que el recuadro de selección “The key is provided for me automatically” (La clave me es proporcionada automáticamente) que se encuentra en la parte inferior no esté marcado. Si está utilizando este ordenador para conectarse a la red de una empresa, consulte con su administrador de red si es necesario marcar esta casilla.
5. Introduzca su clave WEP en el recuadro “Network key” (Clave de red).

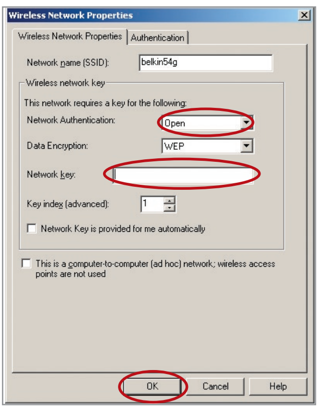


Importante: Una clave WEP es una mezcla de números y letras de la A a la F y del 0 al 9. Para WEP de 128 bits, deberá introducir 26 claves. Para WEP de 64 bits, deberá introducir 10 claves. Esta clave de red deberá coincidir con la clave que haya asignado a su router inalámbrico o punto de acceso.

6. Haga clic en “OK” para guardar los ajustes.

Conexión de su ordenador a una red inalámbrica que requiera WPA-PSK (sin servidor)

1. Haga doble clic sobre este icono de “Indicador de señal” para abrir la pantalla “Wireless Network” (Utilidad de red inalámbrica). El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta inalámbrica.
2. En la pestaña “Wireless Network” (Redes inalámbricas), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
3. En “Network Authentication” (Autenticación de red), seleccione “WPA-PSK (No Server)”.
4. Introduzca su clave WEP en el recuadro “Network key” (Clave de red).

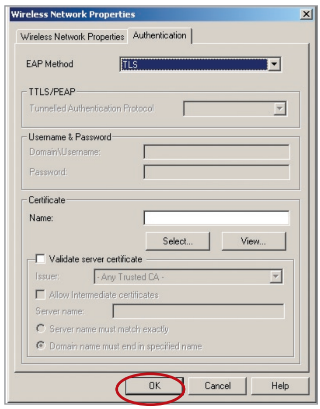


Importante: WPA-PSK es una combinación de números y letras de la A a la Z y del 0 al 9. Para WPA-PSK, puede introducir de ocho a 63 caracteres. Esta clave de red deberá coincidir con la clave que haya asignado a su router inalámbrico o punto de acceso.

5. Haga clic en “OK” para guardar los ajustes.

Conexión de su ordenador a una red inalámbrica que requiera WPA (con servidor Radius)

1. Haga doble clic sobre este icono de "Indicador de señal" para abrir la pantalla "Wireless Network" (Utilidad de red inalámbrica). El botón "Advanced" (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta inalámbrica.
2. En la pestaña "Wireless Network" (Redes inalámbricas), seleccione un nombre de red de la lista "Available networks" (Redes disponibles) y haga clic en "Configure" (Configurar).
3. En "Network Authentication" (Autenticación de red), seleccione "WPA".
4. En la pestaña "Authentication" (Autenticación), seleccione las configuraciones indicadas por su administrador de red.
5. Haga clic en "OK" para guardar los ajustes.



Configuración de WPA/WPA2 para tarjetas de red inalámbrica para ordenador portátil y de sobremesa que no sean de Belkin

En el caso de las tarjetas de red inalámbrica para ordenadores de sobremesa y portátiles que no sean de Belkin y que no estén equipadas con un software compatible con WPA/WPA2, se puede descargar de forma gratuita un archivo de Microsoft llamado "Windows XP Support Patch for Wireless Protected Access" (actualización de soporte Windows XP para acceso inalámbrico protegido)

Atención: El archivo que Microsoft pone a su disposición sólo funciona con Windows XP. En la actualidad no existe soporte para otros sistemas operativos.

Importante: Asimismo, deberá asegurarse de que el fabricante de la tarjeta inalámbrica soporte WPA/WPA2 y de haber descargado e instalado el controlador más actualizado de su página de asistencia.

Sistemas operativos compatibles: • **Windows XP Professional**

• **Windows XP Home Edition**

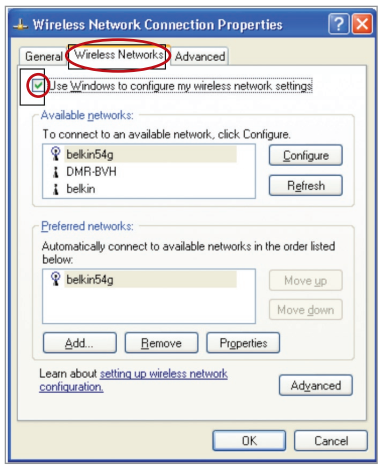
Configuración de la utilidad de red inalámbrica de Windows XP para emplear WPA/WPA2-PSK

Para utilizar WPA-PSK, asegúrese de que está utilizando la Utilidad de Red Inalámbrica de Windows. Para ello, debe seguir los siguientes pasos:

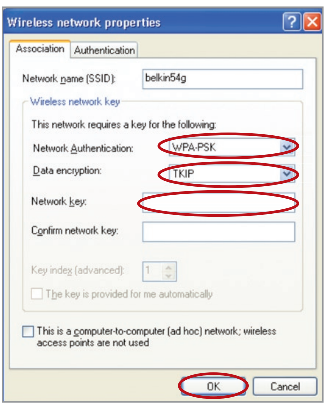
1. En Windows XP, haga clic sobre "Start > Control Panel > Network Connections" (Inicio > Panel de Control > Conexiones de Red).

2. Haga clic con el botón derecho del ratón sobre "Wireless Network Connection" (Conexión de red inalámbrica) y seleccione "Properties" (Propiedades)

3. Al hacer clic en la pestaña "Wireless Networks" (Redes inalámbricas), aparecerá la siguiente pantalla. Compruebe que esté marcada la casilla "Use Windows to configure my wireless network settings" (Utilizar Windows para configurar mis ajustes de red inalámbrica).



4. En la pestaña "Wireless Networks" (Redes inalámbricas), haga clic sobre el botón "Configure" (Configurar) y aparecerá la siguiente pantalla.



5. Para usuarios de redes para casa u oficinas pequeñas, seleccione "WPA-PSK" o "WPA2-PSK" en "Network Authentication" (Autenticación de red).

Nota: Seleccione WPA si está utilizando este ordenador para conectarse a una red corporativa que soporte un servidor de autenticación como el servidor Radius. Consulte con su administrador de red para obtener más información.

6. Para la encriptación de datos (“Data Encryption”), seleccione “TKIP” o “AES”. Este ajuste deberá ser idéntico al del router que instale.

7. Introduzca su clave de encriptación en el recuadro “Network key” (Clave de red).

Importante: Introduzca su clave precompartida. Puede estar compuesta por entre ocho y 63 caracteres entre letras, números y símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale.

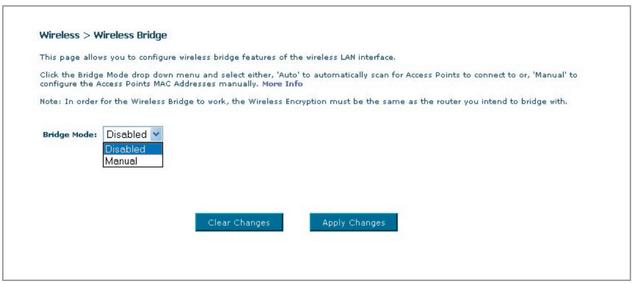
8. Haga clic en “OK” para aplicar los ajustes.

Puente inalámbrico

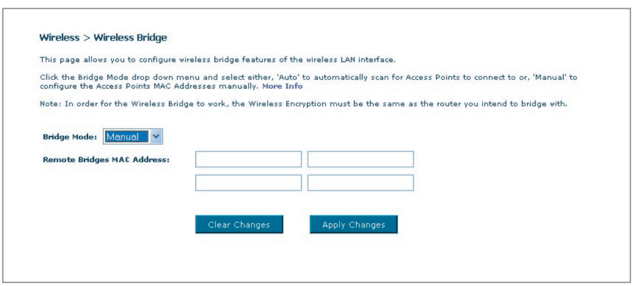
El Puenteo inalámbrico o Sistema de distribución inalámbrica (WDS) se emplea para conectar routers inalámbricos con puntos de acceso inalámbricos para ampliar una red.

Haga clic en el menú desplegable que se encuentra junto a “Modo de puenteo” para seleccionar una de las siguientes opciones:

Desactivado: Para desactivar el puenteo inalámbrico (predeterminado)



Manual: Ingreso manual de la(s) dirección(es) MAC de los puntos de acceso.



1 Los canales inalámbricos del router y punto de acceso deben coincidir.

2 Los ajustes de seguridad (WEP) del router y punto de acceso deberán coincidir.

3 Si está activado el filtro de direcciones MAC, el usuario deberá asegurarse de añadir la(s) dirección(es) MAC de WLAN del router/PA con el fin de permitir la comunicación entre los mismos.

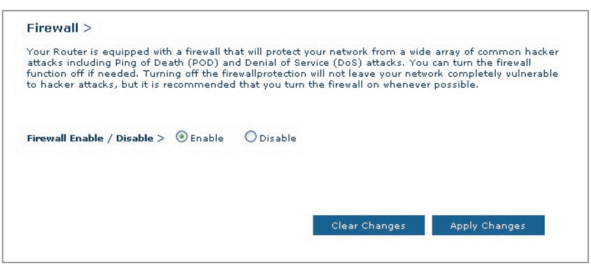
4 Si está utilizando una red que está protegida con seguridad WPA, la SSID en ambos puntos de acceso deberá coincidir.

Firewall

Su router se encuentra equipado con un firewall que protegerá su red de una amplia gama de ataques habituales de piratas informáticos, incluyendo:

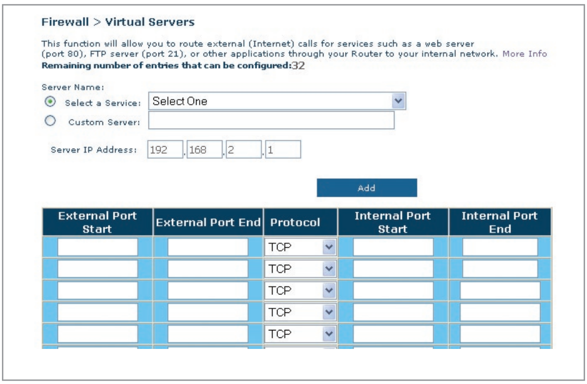
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS, Denegación de servicio)
- IP con longitud cero
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

El firewall también protege puertos comunes que son empleados con frecuencia para atacar redes. Estos puertos aparecen como “Stealth” (Invisibles), lo que significa principalmente que estos puertos no existen ante un posible pirata informático. Si lo necesita, puede apagar la función de firewall; sin embargo, se recomienda dejar el firewall activado. Si desactiva la protección por firewall, no dejará su red completamente vulnerable a los ataques de los piratas, pero es recomendable dejar activado el firewall.



Servidores virtuales

Los servidores virtuales le permiten enrutar llamadas externas (Internet) para servicios como servidor web (puerto 80), servidor FTP (puerto 21) y otras aplicaciones a través de su router hasta su red interna. Gracias a que sus ordenadores internos están protegidos por un firewall, las máquinas fuera de su red (a través de Internet) no pueden acceder a ellos, ya que no pueden ser 'vistos'. Si necesita configurar el servidor virtual para una aplicación específica, será preciso que se ponga en contacto con el fabricante de la aplicación para descubrir los ajustes de los puertos precisos. Podrá introducir esta información de puerto en su router de manera manual.



Selección de una aplicación

Se ha incluido una lista de aplicaciones comunes de la que seleccionar. Haga clic en "Select a Service" y luego seleccione una aplicación del menú desplegable. Los ajustes serán transferidos a la primera fila que haya especificado. Haga clic en "Add" para guardar el ajuste para esta aplicación.

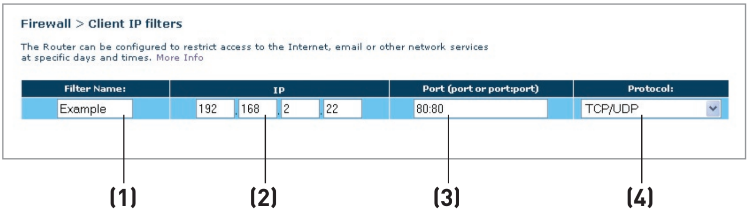
Introducción manual de los ajustes en el Servidor Virtual

Para introducir los ajustes manualmente, haga clic en "Custom Server" e ingrese un nombre para el servidor. Introduzca la dirección IP del servidor en el espacio provisto para la máquina interna (servidor) y el puerto o los puertos necesarios para pasar. Luego, seleccione el tipo de protocolo (TCP o UDP) y haga clic en "Add".

Abrir los puertos de su firewall puede representar un riesgo para la seguridad. Puede activar y desactivar los ajustes con gran rapidez. Se recomienda desactivar las configuraciones cuando no esté utilizando una aplicación específica.

Filtros para IP de clientes

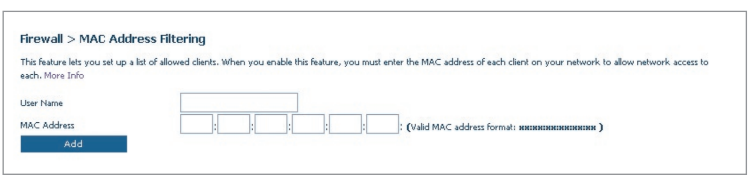
El router puede ser configurado para restringir el acceso a Internet, al e-mail o a otros servicios de red en determinados días y horas.



Para restringir el acceso a Internet a un único ordenador, introduzca el nombre del filtro en el recuadro de “Filter Name” **(1)** y la dirección de IP del ordenador para el cual desea restringir el acceso en el campo de IP **(2)**. A continuación, introduzca “80” en ambos campos de puerto **(3)**. Seleccione el protocolo en el recuadro desplegable “Protocol” **(4)**. Haga clic sobre “Apply Changes” (Aplicar cambios). A partir de ahora, el acceso a Internet estará bloqueado para el ordenador y la dirección IP que ha especificado.

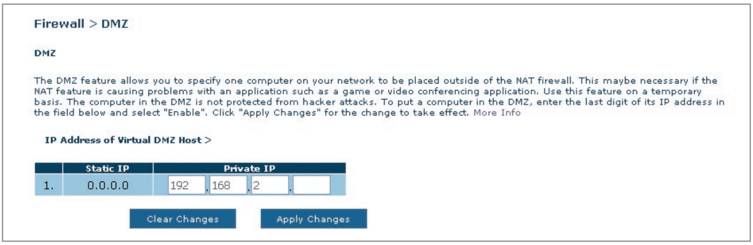
Filtrado de direcciones MAC

El filtro de direcciones MAC es una potente característica de seguridad que le permite especificar qué ordenadores están permitidos en la red. Cualquier ordenador que trate de acceder a la red y no esté especificado en la lista de filtrado no obtendrá permiso para acceder. Cuando active esta propiedad, deberá introducir un nombre de usuario y la dirección MAC de cada cliente de su red para permitir el acceso a la misma de cada uno de ellos. Luego, haga clic sobre “Add” para guardar la configuración.



DMZ (Zona desmilitarizada)

Si uno de los clientes conectados no puede llevar a cabo una aplicación de Internet correctamente debido al firewall, podrá establecer un acceso a Internet no restringido en ambas direcciones para dicho ordenador. Esto puede ser necesario en el caso de que la propiedad NAT esté causando problemas con una aplicación como, por ejemplo, una aplicación de juegos o de videoconferencia. Utilice esta característica de forma temporal. **El ordenador que se encuentra en la DMZ no está protegido contra los ataques de piratas informáticos.**

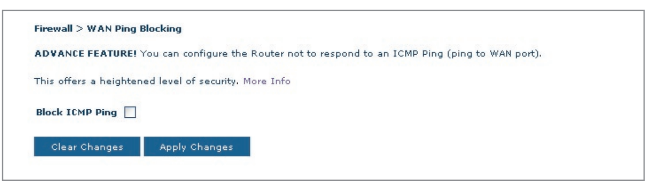


Para establecer una zona desmilitarizada para uno de los ordenadores, introduzcae la dirección IP del ordenador en el campo “Private IP” (IP privada) y haga clic en “Apply Changes” (Aplicar cambios) para activar los ajustes.

Bloqueo de un ICMP Ping

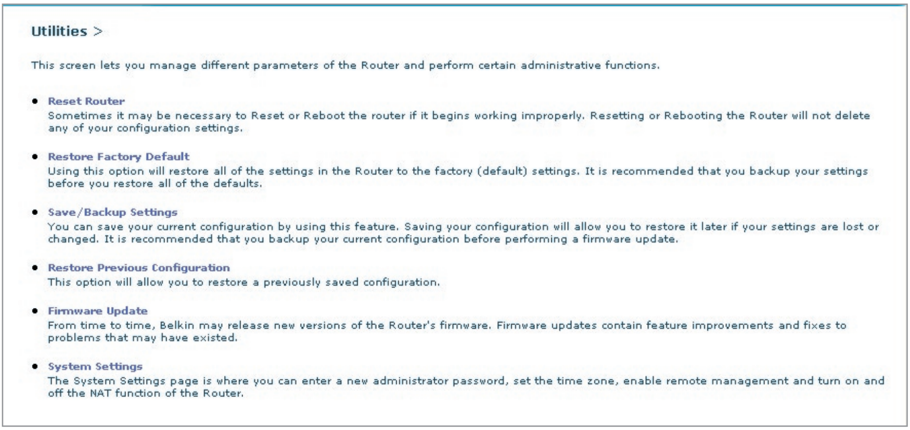
Los piratas informáticos utilizan lo que se conoce como “pinging” (revisar actividad) para encontrar víctimas potenciales en Internet. Al revisar la actividad de una dirección IP específica y recibir una respuesta de la dirección IP, el pirata informático puede determinar si hay allí algo de interés. El router puede ser configurado de forma que no responda a un ICMP ping proveniente del exterior. Esto eleva el nivel de seguridad de su router.

Para apagar la respuesta al ping, seleccione “Block ICMP Ping” (bloquear ICMP ping) **(1)** y haga clic en “Apply Changes” (aplicar cambios). El router no responderá a ningún ICMP ping.



Utilidades

La pantalla de "Utilities" (Utilidades) le permite gestionar diferentes parámetros del router y llevar a cabo determinadas funciones administrativas.



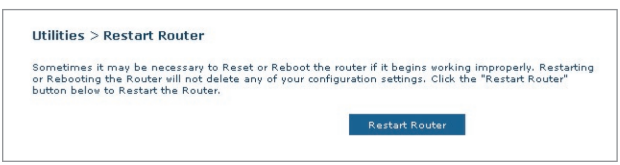
Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Reset Router**
  Sometimes it may be necessary to Reset or Reboot the router if it begins working improperly. Resetting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Default**
  Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Settings**
  You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Configuration**
  This option will allow you to restore a previously saved configuration.
- **Firmware Update**
  From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
- **System Settings**
  The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the NAT function of the Router.

Reiniciar el router

Algunas veces es posible que sea necesario reiniciar el router en caso de que comience a funcionar mal. Al reiniciar el router NO se borrará ninguno de sus ajustes de configuración.



Utilities > Restart Router

Sometimes it may be necessary to Reset or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.

Restart Router

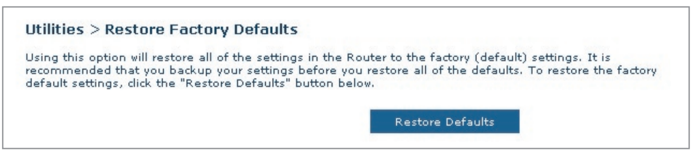
Reinicio del router para restablecer el funcionamiento normal

1. Haga clic en el botón “Restart Router” (Reiniciar router).
2. Aparecerá el siguiente mensaje. Haga clic en “Yes” (Sí) para reiniciar su router.

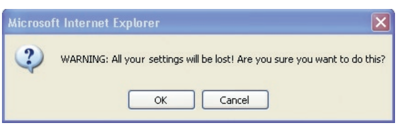


Restablecer las configuraciones por defecto de fábrica

El empleo de esta opción restablecerá los ajustes (predeterminados) de fábrica del router. Se recomienda que realice una copia de seguridad de sus ajustes antes de restablecer todos los ajustes por defecto.

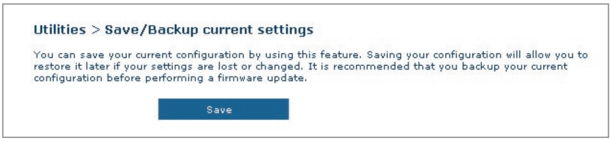


1. Haga clic en el botón “Restore Defaults” (Restablecer ajustes por defecto).
2. Aparecerá el siguiente mensaje. Haga clic en “OK” (Aceptar) para restablecer las configuraciones por defecto de fábrica.

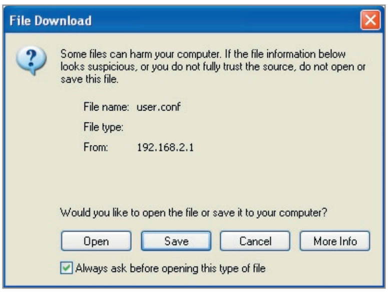


Guardar/Copia de seguridad de ajustes actuales

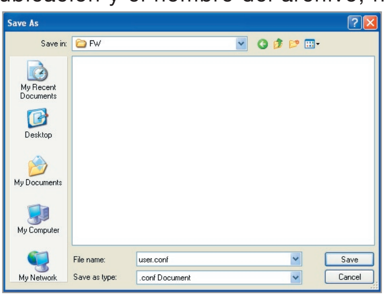
Puede guardar su configuración actual utilizando esta función. El guardar su configuración le permitirá restablecerla posteriormente, en caso de que sus ajustes se pierdan o se modifiquen. Se recomienda realizar una copia de seguridad de su configuración actual antes de llevar a cabo una actualización del firmware.



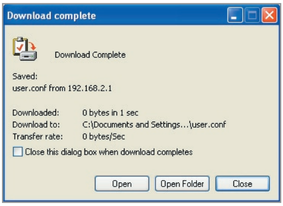
1. Haga clic en “Save” (Guardar). Se abrirá una ventana llamada “File Download” (descarga de archivos). Haga clic en “Save” (Guardar).



2. Se abrirá una ventana que le permitirá seleccionar la ubicación en la que desea guardar el archivo de configuración. Seleccione una ubicación. No existen restricciones con respecto al nombre del archivo. Sin embargo, asegúrese de dar un nombre al archivo que le permita encontrarlo más tarde. Cuando haya ingresado la ubicación y el nombre del archivo, haga clic en “Save” (Guardar).



3. Cuando el proceso de almacenamiento se haya completado, verá la siguiente ventana.
Haga clic en "Close" (Cerrar).

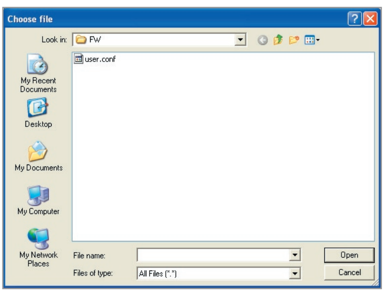


La configuración ha sido guardada.

Restore Previous Settings (Restablecer ajustes anteriores)

Esta opción le permitirá restablecer una configuración guardada anteriormente.

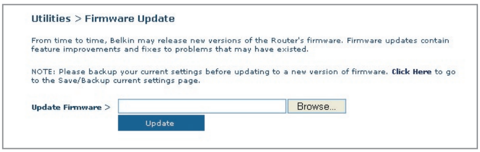
1. Haga clic en "Browse" (Examinar). Se abrirá una ventana que le permitirá seleccionar la ubicación del archivo de configuración. Todos los archivos de configuración presentan la extensión ".conf". Localice el archivo de configuración que desea restablecer y haga doble clic sobre él.



2. Haga clic en "Open". (Abrir).

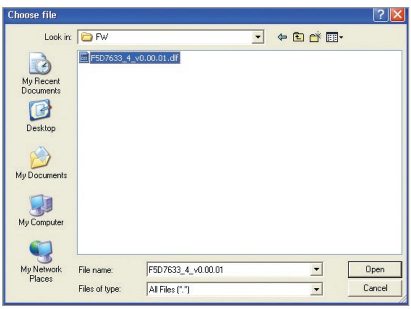
Actualización del firmware

Cada cierto tiempo, Belkin publica nuevas versiones del firmware del router. Las actualizaciones del firmware contienen mejoras de las propiedades y soluciones para los problemas que puedan haber existido. Cuando Belkin publique un nuevo firmware, usted podrá descargarlo de la página web de actualizaciones de Belkin con el fin de instalar la versión más actualizada del firmware de su router.



Actualización del firmware del router

1. En la ventana "Firmware Update" (Actualización del firmware), haga clic en "Browse" (Examinar) Se abrirá una ventana que le permitirá seleccionar la ubicación del archivo de actualización del firmware.



2. Navegue hasta llegar al archivo de firmware descargado. Seleccione el archivo haciendo doble clic en el nombre del mismo.

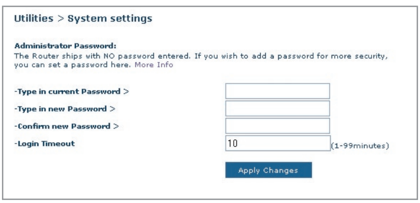
3. Haga clic en "Update" (Actualizar) para instalar la versión más actual de firmware.

Ajustes del sistema

La página “System Settings” (Ajustes del sistema) es en donde podrá introducir una nueva contraseña de administrador, establecer la zona horaria, activar la gestión a distancia y encender y apagar la función UPnP del router.

Establecimiento o modificación de la contraseña del administrador

El router efectúa el envío SIN necesidad de introducir contraseña. Si desea añadir una contraseña para disfrutar de una mayor seguridad, puede establecerla aquí. Escriba su contraseña y guárdela en un lugar seguro, ya que la necesitará si precisa acceder al router en el futuro. Se recomienda asimismo que establezca una contraseña si prevé utilizar la opción de gestión a distancia de su router.



Modificación del tiempo límite de acceso

La opción de tiempo límite de acceso le permite establecer el periodo de tiempo que podrá permanecer en la interfaz de configuración avanzada del router. El temporizador se inicia cuando deja de detectarse actividad. Por ejemplo, usted ha efectuado algunos cambios en la interfaz de configuración avanzada y después deja su ordenador solo sin hacer clic en “Logout” (Salir). Si suponemos que el tiempo límite es de 10 minutos, entonces 10 minutos después de que abandone el ordenador, la sesión se cerrará. Deberá acceder al router de nuevo para realizar más cambios. La opción del tiempo límite de acceso responde a razones de seguridad y el tiempo predeterminado es de 10 minutos.

Atención: Solamente podrá acceder un ordenador cada vez a la interfaz de configuración avanzada del router.

Establecimiento de la hora y de la zona horaria

El router mantiene la hora conectándose a un servidor SNTP (Simple Network Time Protocol, protocolo horario de red simple). Esto permite al router sincronizar el reloj del sistema con la red global de Internet. El reloj sincronizado en el router se utiliza para grabar el registro de seguridad y controlar el filtro de clientes.

Seleccione los servidores NTP correspondientes y la zona horaria en la que reside y haga clic en "Apply Changes" (Aplicar cambios). Puede que el reloj del sistema no se actualice de forma inmediata. Espere al menos 15 minutos para que el router contacte con los servidores horarios de Internet y obtenga una respuesta. No puede cambiar el reloj por su cuenta.



Activación de la gestión a distancia

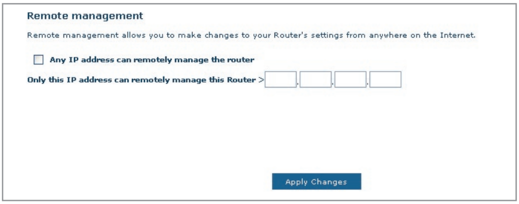
Antes de activar esta función avanzada de su router de Belkin, **ASEGÚRESE DE QUE HA ESTABLECIDO LA CONTRASEÑA DE ADMINISTRADOR.** La gestión a distancia le permite efectuar cambios en los ajustes de su router desde cualquier parte en Internet.

Haga clic en el botón "Change Settings" (Modificar ajustes) para abrir la ventana "Remote Management" (Gestión a distancia).

Existen dos métodos de gestionar el router a distancia. El primero consiste en permitir el acceso al router desde cualquier parte en Internet seleccionando la opción "Any IP address can remotely manage the Router" (cualquier dirección IP puede gestionar el router a distancia). Al introducir su dirección IP de WAN desde cualquier ordenador en Internet, aparecerá una ventana de acceso en la que deberá introducir la contraseña de su router.

El segundo método consiste en permitir la gestión a distancia únicamente a una dirección IP específica. Este método es más seguro pero menos cómodo. Para utilizar este método, introduzca la dirección IP desde la que vaya a acceder al router en el espacio previsto y seleccione "Only this IP address can remotely manage the Router" (únicamente esta dirección IP puede gestionar el router a distancia). Antes de activar esta función, se RECOMIENDA ENCARECIDAMENTE que establezca su contraseña de administrador. Si deja la contraseña vacía, dejará su router expuesto a posibles intrusiones.

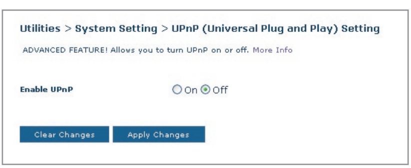
Haga clic en “Apply Changes” (Aplicar cambios) para guardar los ajustes.



Activar/Desactivar UPnP

El UPnP (plug-and-play universal) es una propiedad avanzada adicional que ofrece su Router de Belkin. Es una tecnología que ofrece un funcionamiento perfecto de las opciones de mensajes de voz, mensajes de vídeo, juegos y otras aplicaciones compatibles con UPnP. Algunas aplicaciones requieren que el firewall del router sea configurado de una forma específica para funcionar correctamente. Normalmente requiere la apertura de puertos TCP y UDP y, en algunos casos, el establecimiento de puertos de activación. Una aplicación compatible con UPnP tiene la capacidad de comunicarse con el router, básicamente “diciendo” al router la forma en que necesita que sea configurado el firewall. El router que se le ha suministrado viene con la función UPnP desactivada. Si está utilizando cualquier aplicación compatible con UPnP y desea sacar partido de las características UPnP, puede activar la característica UPnP.

Haga clic en el botón “Change Settings” (Modificar ajustes) para abrir la ventana “UPnP Setting” (Configuración de UPnP). Luego, seleccione “On” para “Enable UPnP” (Activar UPnP). Haga clic en “Apply Changes” (Aplicar cambios) para guardar los ajustes.



Problema:

El LED de ADSL no está encendido.

Solución:

1. Verifique la conexión entre el router y la línea ADSL. Asegúrese de que el cable de la línea ADSL se encuentre conectado al puerto del router con la etiqueta “DSL Line”.
2. Asegúrese de que el router disponga de alimentación. El LED ⏻ de la alimentación ubicado en el panel frontal debe estar iluminado.

Problema:

El LED de Internet no está encendido.

Solución:

1. Asegúrese de que el cable de la línea ADSL se encuentre conectado al puerto del router con la etiqueta “DSL Line”.y que el LED de ADSL esté iluminado.
2. Asegúrese de haber ingresado los datos correctos para VPI/VCI, nombre del usuario y contraseña, suministrados por su ISP.

Problema:

Mi tipo de conexión es “static IP address” (dirección IP estática). No puedo conectar a Internet.

Solución:

Debido a que su tipo de conexión es “static IP address” (dirección IP estática), su ISP deberá asignarle la dirección IP, máscara de subred y dirección de gateway (pasarela). En vez de utilizar el asistente de instalación, vaya al menú de “Connection Type” (Tipo de conexión) y seleccione el tipo de conexión correspondiente. Luego, haga clic en “Next” (Siguiente), seleccione “Static IP” (IP estática), e introduzca la información de máscara de subred y dirección de gateway (pasarela).

Problema:

He olvidado o perdido mi contraseña.

Solución:

Presione y mantenga presionado el botón “Reset” (Reinicio), ubicado en el panel frontal, durante al menos diez segundos. De esta manera, restablecerá los ajustes de fábrica por defecto.

Problema:

Mi ordenador no puede conectarse de manera inalámbrica al router.

Solución:

1. Asegúrese de que su PC inalámbrico tenga los mismos ajustes SSID que el router y de tener los mismos ajustes de seguridad, como la encriptación WPA o WEP, en los clientes.
2. Asegúrese de que el router y el PC inalámbrico no estén demasiado lejos el uno del otro.

Problema:

La red inalámbrica es interrumpida con frecuencia.

Solución:

1. Coloque su PC inalámbrico más cerca del router para encontrar una mejor señal.
2. También es posible que haya interferencias, causadas posiblemente por un horno microondas o teléfonos de 2.4GHz. Coloque el router en otro lugar o utilice un canal inalámbrico diferente.

Problema:

No puedo conectar a Internet de forma inalámbrica.

Solución:

Si no puede conectarse a Internet desde un ordenador inalámbrico, compruebe lo siguiente:

1. Contemple las luces de su router. Si está utilizando un router de Belkin, los indicadores LED deberán tener el siguiente aspectol:
   - El indicador LED de alimentación deberá estar encendido.
   - El indicador LED de DSL deberá estar encendido pero no intermitente.
   - El indicador LED de Internet deberá estar encendido o intermitente.
2. Abra el software de su utilidad inalámbrica haciendo clic en el icono de la bandeja del sistema en la esquina inferior derecha de la pantalla. Si está utilizando una Tarjeta Inalámbrica de Belkin, el ícono de la bandeja tendrá el siguiente aspecto.   El icono puede estar rojo o verde.
3. La ventana exacta que aparece variará dependiendo del modelo de tarjeta inalámbrica del que disponga; sin embargo, todas las utilidades deberán presentar una lista de “Redes Disponibles”; aquellas redes inalámbricas a las que se puede conectar.

¿Aparece en los resultados el nombre de su red inalámbrica?

Sí, el nombre de mi red aparece en la lista, entonces, consulte la solución de problemas “No puedo conectar a Internet de forma inalámbrica pero el nombre de mi red aparece en la lista”.

No, el nombre de mi red no aparece en la lista. Entonces, consulte la solución de problemas “No puedo conectar a Internet de forma inalámbrica y el nombre de mi red no aparece en la lista”.

Problema:

No puedo conectar a Internet de forma inalámbrica pero el nombre de mi red aparece en la lista.

Solución:

Si el nombre de su red aparece en la lista “Available Networks” (Redes Disponibles), siga los siguientes pasos para realizar la conexión inalámbrica:

1. Haga clic en el nombre correcto de la red en la lista de “Available Networks” (redes disponibles).
2. Si la red tiene activada la seguridad (encriptación), deberá introducir la clave de red. Para más información acerca de la seguridad, consulte la página titulada: “Modificación de los ajustes de encriptación inalámbrica”.
3. En pocos segundos, el icono de la bandeja del sistema, en la esquina inferior izquierda de su pantalla, deberá ponerse de color verde indicando la correcta conexión con la red.



Problema:

No puedo conectar a Internet de forma inalámbrica y el nombre de mi red no aparece en la lista.

Solución

Si el nombre correcto de la red no aparece en la lista “Available Networks” (Redes Disponibles) en la utilidad inalámbrica, intente realizar los siguientes pasos para la resolución del problema:

1. Desplace temporalmente el ordenador, si es posible, a una distancia de 3 metros del router. Cierre la utilidad inalámbrica y vuelva a abrirla. Si ahora aparece el nombre correcto de la red en

la lista “Redes Disponibles”, es posible que tenga un problema de alcance o de interferencia. Consulte las sugerencias incluidas en el Anexo B, “Factores importantes para la colocación y configuración”.

2. Empleando un ordenador que esté conectado al router a través de un cable de red (al contrario que de forma inalámbrica), asegúrese de que esté activado “Broadcast SSID” (emitir SSID). Esta configuración se encuentra en la página de configuración inalámbrica titulada “Channel and SSID” (Canal y SSID).

Si aún no puede acceder a Internet después de completar estos pasos, póngase en contacto con el servicio de asistencia técnica de Belkin.

Problema:

El rendimiento de mi red inalámbrica es irregular.

La transferencia de datos es lenta en ocasiones.

La potencia de la señal es débil.

Dificultad para establecer y/o mantener una conexión de red privada virtual (VPN, Virtual Private Network).

Solución:

La tecnología inalámbrica está basada en la radioemisión, lo que significa que la conectividad y el rendimiento entre dispositivos descenderán a medida que aumente la distancia entre los mismos. Otros factores que provocan un debilitamiento de la señal (el metal es habitualmente el responsable) son obstáculos como paredes y aparatos metálicos. Como resultado, el alcance habitual de sus dispositivos inalámbricos en interiores se situará entre 30 y 60 m. Tenga en cuenta, además, que la velocidad de conexión puede verse mermada cuando más se aleje del router (o punto de acceso).

Con el fin de determinar si los problemas de conexión inalámbrica están relacionados con el alcance, le sugerimos que desplace provisionalmente el ordenador, a ser posible, a una distancia de entre 1,5 y 3 m del router.

Cambio del canal inalámbrico:según la interferencia y el tráfico inalámbrico del área, cambiar el canal inalámbrico de su red puede mejorar el rendimiento y la fiabilidad. El canal 11 es el canal predeterminado con el que se suministra el router. Puede elegir entre

varios canales dependiendo de su región; consulte la página 37 "modificación del canal inalámbrico" para obtener instrucciones de cómo elegir otros canales.

Limitación de la velocidad de transmisión inalámbrica: Limitar la velocidad de transmisión inalámbrica puede ayudar a mejorar la estabilidad de la conexión y el alcance inalámbrico máximo. La mayoría de las tarjetas inalámbricas tiene la capacidad de limitar la velocidad de transmisión. Para cambiar esta propiedad, vaya al panel de control de Windows, abra la ventana "Conexiones de red" y haga doble clic sobre la conexión de su tarjeta inalámbrica. En el diálogo de propiedades, seleccione el botón "Configure" (Configurar) en la pestaña "General" (los usuarios de Windows 98 deberán seleccionar la tarjeta inalámbrica en el cuadro de lista y luego hacer clic sobre "Properties" [Propiedades]), y luego elija la pesta-a "Advanced" (Opciones Avanzadas) y seleccione la propiedad de velocidad. Por lo general, las tarjetas de cliente inalámbrico se configuran de forma automática para ajustar la velocidad de transmisión inalámbrica, pero esto puede causar interrupciones periódicas en la conexión si la señal inalámbrica es demasiado débil. Como regla general, las velocidades de transmisión más lentas son más estables. Experimente con diferentes velocidades de conexión hasta que encuentre la mejor para su entorno, tome nota de que todas las velocidades de transmisión disponibles deben ser aceptables para navegar por Internet. Para obtener mayor asesoría, consulte el manual del usuario de su tarjeta inalámbrica.

Problema:

Tengo dificultades para configurar la WEP (Wired Equivalent Privacy, privacidad equivalente a la del cable) en un router de Belkin o punto de acceso de Belkin.

Solución

1. Acceda a su router inalámbrico o punto de acceso.
2. Abra su navegador de Internet e introduzca la dirección IP del router inalámbrico o punto de acceso. (La dirección IP pre-determinada del router es 192.168.2.1 y la dirección IP del punto de acceso 802.11g es 192.168.2.254). Acceda a su router haciendo clic en el botón "Login" (Acceso) de la parte superior derecha de la pantalla. Se le solicitará que introduzca su contraseña. Si nunca antes ha establecido una contraseña, deje en blanco el campo de contraseña y haga clic sobre "Submit" (Enviar).
3. Haga clic en la pestaña "Wireless" (Inalámbrico) situada en la parte izquierda de su pantalla. Seleccione la pestaña "Encryption" (Encriptación) o "Security" (Seguridad) para acceder a la pantalla de ajustes de seguridad.
4. Seleccione "128-bit WEP" (WEP de 128 bits) del menú desplegable.
5. Después de seleccionar su modo de encriptación WEP, podrá introducir su clave WEP hexadecimal manualmente, o introducir una frase de paso en

el campo “Passphrase” y hacer clic en “Generate” (generar) para crear una clave WEP a partir de la frase de paso. Haga clic en “Apply Changes” (Aplicar cambios) para finalizar. Ahora deberá hacer que todos sus clientes coincidan con estos ajustes. Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9. Para la WEP de 128 bits deberá introducir 26 claves hexadecimales.

Por ejemplo:
C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = clave de 128 bits

6. Haga clic en “Apply Changes” (aplicar cambios) para finalizar. Ahora está establecida la encriptación en el router inalámbrico. Cada ordenador de su red inalámbrica deberá ser configurado ahora con los mismos ajustes de seguridad.

ATENCIÓN: Si está configurando el router inalámbrico o punto de acceso desde un ordenador con un cliente inalámbrico, necesitará asegurarse de que el modo de seguridad esté activado para este cliente inalámbrico. De lo contrario, perderá su conexión inalámbrica.

Nota para los usuarios de Mac: Los productos originales Apple AirPort® soportan exclusivamente la encriptación de 64 bits. Los productos Apple AirPort 2 soportan la encriptación de 64 o de 128 bits. Compruebe qué versión del producto Apple AirPort está utilizando. Si no puede configurar su red con una encriptación de 128 bits, pruebe con una encriptación de 64 bits.

Problema:

Tengo dificultades para configurar la WEP (Wired Equivalent Privacy, privacidad equivalente a la del cable) en una tarjeta inalámbrica de cliente de Belkin.

Solución:

La tarjeta inalámbrica deberá emplear la misma clave que el router inalámbrico o punto de acceso. Por ejemplo, si su router inalámbrico o punto de acceso utilizan la clave 00112233445566778899AABBCC, la tarjeta inalámbrica debe ser configurada con la misma clave.

1. Haga doble clic en el icono de indicador de señal para abrir la pantalla de red inalámbrica. El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su Tarjeta.
2. El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su Tarjeta.
3. Cuando haga clic en el botón “Advanced” (Avanzado) aparecerá la utilidad de LAN inalámbrica de Belkin. Esta utilidad le permitirá gestionar todas las propiedades avanzadas de la tarjeta inalámbrica de Belkin.
4. En la pestaña “Wireless Network Properties” (Redes inalámbricas: propiedades),

seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).

5. En la categoría “Data Encryption” (Encriptación de datos), seleccione “WEP”.
6. Asegúrese de que el recuadro de selección “The key is provided for me automatically” (La clave me es proporcionada automáticamente) que se encuentra en la parte inferior no esté marcado. Si está utilizando este ordenador para conectarse a la red de una empresa, consulte con su administrador de red si es necesario marcar esta casilla.
7. Introduzca su clave WEP en el recuadro “Network key” (Clave de red).

   Importante: Una clave WEP es una mezcla de números y letras de la A a la F y del 0 al 9. Para WEP de 128 bits, deberá introducir 26 claves. Esta clave de red deberá coincidir con la clave que haya asignado a su router inalámbrico o punto de acceso.

   Por ejemplo: **C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4** = clave de 128 bits
8. Haga clic en “OK” y después “Apply” (Aplicar) para guardas los ajustes.

Si **NO** está utilizando una tarjeta de cliente inalámbrica de Belkin, consulte el manual del usuario del fabricante de la tarjeta de cliente inalámbrica que esté utilizando.

Problema:

¿Soportan los productos Belkin la seguridad WPA?

Solución

Nota: Para utilizar la seguridad WPA, todos sus clientes deberán haber actualizado los controladores y el software compatibles. En el momento de la publicación de esta sección de Preguntas Frecuentes (FAQ), se puede descargar de Microsoft un parche de seguridad gratuito. Este parche sólo funciona con el sistema operativo Windows XP.

Descargue el parche en la siguiente dirección:

http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

Asimismo, deberá descargar el controlador más actualizado para su tarjeta de red inalámbrica 802.11g para portátil o para ordenador de sobremesa de Belkin desde la página de asistencia de Belkin. En la actualidad no existe soporte para otros sistemas operativos. El parche de Microsoft sólo es compatible con dispositivos con controladores preparados para WPA, como los productos 802.11g de Belkin.

Descargue el driver más actual aquí:
http://web.belkin.com/support/networkingsupport.asp.

El soporte para WPA será instalado automáticamente al actualizar su sistema con el Windows XP Service pack 2. Para obtener más detalles, consulte

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en un router de Belkin o punto de acceso de Belkin para una red de hogar.

Solución:

1. Desde el menú desplegable del modo de seguridad (“Security mode”), seleccione “WPA-PSK (no server)” (WPA-PSK, sin servidor).
2. Para la técnica de encriptación (“Encryption Technique”), seleccione “TKIP” o “AES”. Este ajuste deberá ser idéntico en todos los clientes que instale.
3. Introduzca su clave precompartida. Puede estar compuesta por entre 8 y 63 caracteres entre letras, números y símbolos o espacios. Esta misma clave deberá ser utilizada en todos los clientes que instale. Por ejemplo, su PSK será algo así como: “Clave de red familia Pérez”.
4. Haga clic en “Apply Changes” (aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en un router de Belkin o punto de acceso de Belkin para un negocio.

Solución:

Si su red emplea un servidor Radius para distribuir las claves a los clientes, utilice este ajuste. Se emplea habitualmente en un entorno empresarial.

1. Desde el menú desplegable del modo de seguridad (“Security mode”), seleccione “WPA-Radius server” (WPA - Servidor Radius).
2. Para la técnica de encriptación (“Encryption Technique”), seleccione “TKIP” o “AES”. Este ajuste deberá ser idéntico en todos los clientes que instale.
3. Introduzca la dirección IP del servidor Radius en los campos de “Radius Server”.
4. Introduzca la clave Radius en el campo “Radius Key”.
5. Introduzca el intervalo de la clave. El intervalo de clave es la frecuencia con la que se distribuyen las claves (en paquetes).
6. Haga clic en “Apply Changes” (aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en una tarjeta de cliente inalámbrico de Belkin para una red de hogar.

Solución:

Los clientes deberán emplear la misma clave que el router inalámbrico G o punto de acceso. Por ejemplo, si la clave es “clave red familia Smith” en el router inalámbrico o punto de acceso, el cliente también debe utilizar esa misma clave.

1. Haga doble clic sobre este icono de “Indicador de señal” para abrir la pantalla “Wireless Network” (Utilidad de red inalámbrica). El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta.
2. El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su Tarjeta.
3. Cuando haga clic en el botón “Advanced” (Avanzado) aparecerá la utilidad de LAN inalámbrica de Belkin. Esta utilidad le permitirá gestionar todas las propiedades avanzadas de la tarjeta inalámbrica de Belkin.
4. En la pestaña “Wireless Network Properties” (Redes inalámbricas: propiedades), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Properties” (Propiedades).
5. En “Network Authentication” (Autenticación de red), seleccione “WPA-PSK (no server)” (WPA-PSK, sin servidor).
6. Introduzca su clave WEP en el recuadro “Network key” (Clave de red).

Importante: WPA-PSK es una combinación de números y letras de la A a la Z y del 0 al 9. Para WPA-PSK, puede introducir de ocho a 63 caracteres. Esta clave de red deberá coincidir con la clave que haya asignado a su router inalámbrico o punto de acceso.

7. Haga clic en “OK” y después “Apply” (Aplicar) para guardar los ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en una tarjeta de cliente inalámbrico de Belkin para un negocio.

Solución:

1. Haga doble clic sobre este icono de “Indicador de señal” para abrir la pantalla “Wireless Network” (Utilidad de red inalámbrica). El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta.
2. El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su Tarjeta.

3. Cuando haga clic en el botón "Advanced" (Avanzado) aparecerá la utilidad de LAN inalámbrica de Belkin. Esta utilidad le permitirá gestionar todas las propiedades avanzadas de la tarjeta inalámbrica de Belkin.

4. En la pestaña "Wireless Network Properties" (Redes inalámbricas: propiedades), seleccione un nombre de red de la lista "Available networks" (Redes disponibles) y haga clic en "Properties" (Propiedades).

5. En "Network Authentication" (Autenticación de red), seleccione "WPA".

6. En la pestaña "Authentication" (Autenticación), seleccione las configuraciones indicadas por su administrador de red.

7. Haga clic en "OK" y después "Apply" (Aplicar) para guardar los ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en una tarjeta de cliente que **NO** es de Belkin para una red de hogar.

Solución:

Si está utilizando una tarjeta inalámbrica para ordenador de sobremesa o para notebook que **NO** es de Belkin y esta tarjeta no está equipada con un software compatible con WPA, se puede descargar de forma gratuita un archivo de Microsoft llamado "Windows XP Support Patch for Wireless Protected Access" (Actualización de Soporte Windows XP para acceso inalámbrico protegido): Busque el parche de Microsoft en la base de conocimiento para WPA con Windows XP y descárguelo.

Atención: El archivo que Microsoft pone a su disposición sólo funciona con Windows XP. En la actualidad no existe soporte para otros sistemas operativos. "Asimismo, deberá asegurarse de que el fabricante de la tarjeta inalámbrica soporte WPA y de haber descargado e instalado el driver más actualizado de su página de asistencia."

Sistemas operativos soportados:

- Windows XP Professional
- Windows XP Home Edition

Activación de WPA-PSK (sin servidor)

1. En Windows XP, haga clic sobre "Start > Control Panel > Network Connections" (Inicio > Panel de Control > Conexiones de Red).

2. Al hacer clic en la pestaña "Wireless Networks" (Redes inalámbricas), aparecerá la siguiente pantalla. Compruebe que esté marcada la casilla "Use Windows to configure my wireless network settings" (Utilizar Windows para configurar mis ajustes de red inalámbrica).

3. En la pestaña “Wireless Networks” (Redes inalámbricas), haga clic sobre el botón “Configure” (Configurar) y aparecerá la siguiente pantalla.
4. Si es un usuario de hogar u oficina pequeña, seleccione “WPA-PSK” en “Network Authentication” (Autenticación de red).

Atención: Seleccione WPA (con servidor Radius) si está utilizando este ordenador para conectarse a una red corporativa que soporte un servidor de autenticación como el servidor Radius. Consulte a su administrador de red para obtener más información.

5. Para la encriptación de datos (“Data Encryption”), seleccione “TKIP” o “AES”. Este ajuste deberá ser idéntico al del router inalámbrico o punto de acceso que haya configurado.
6. Introduzca su clave de encriptación en el recuadro “Network key” (Clave de red).

Importante: Introduzca su clave precompartida. Puede estar compuesta por entre ocho y 63 caracteres entre letras, números y símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale.

7. Haga clic en “OK” para aplicar los ajustes.

¿Cuál es la diferencia entre 802.11b, 802.11g, G + MIMO y Pre-N?

Actualmente existen cuatro niveles de estándares de interconexión en red inalámbrica, que transmiten datos a velocidades máximas muy diferentes. Todos se basan en la designación 802.11(x), llamada así por el IEEE, el consejo responsable de certificar los estándares de interconexión en red. El estándar de interconexión en red más común, el 802.11b, transmite información a 11 Mbps, 802.11a y 802.11g operan a 54 Mbps, G+ MIMO funciona a 54 Mbps y Pre-N a 108 Mbps.

Tabla de comparación inalámbrica

Tecnología inalámbrica	802.11b	G (802.11g)	G+ (802.11g con HSM)	G+ MIMO(802.11g con MIMO MRC)	Belkin Pre-N (802.11g con True MIMO)
Veloci-dad*	11 Mbps tasa de enlace/línea base	5 veces más rápida que 802.11b*	10 veces más rápida que 802.11b*	10 veces más rápida que 802.11b*	15 veces más rápida que 802.11b*
Frecuencia	Los dispositivos domésticos más comunes tales como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2,4 GHz sin licencia	Los dispositivos domésticos más comunes tales como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2,4 GHz sin licencia	Los dispositivos domésticos más comunes tales como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2,4 GHz sin licencia	Los dispositivos domésticos más comunes tales como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2,4 GHz sin licencia	Los dispositivos domésticos más comunes tales como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2,4 GHz sin licencia
Compatibilidad	Compatible con 802.11g	Compatible con 802.11b/g	Compatible con 802.11b/g	Compatible con 802.11b/g	Compatible con 802.11g u 802.11b
Cobertura*	normalmente de 30 a 60 m* en el interior	Hasta 120 m*	Hasta 210 m*	Hasta 300 m*	Hasta 420 m*
Venta-jas	Larga existencia: tecnología heredada	Gran aceptación para el uso compartido de Internet	Velocidad y cobertura mejoradas	Mejor cobertura y velocidad y alcance consistentes	Tecnología punta: mejor cobertura y transmisión

*La distancia y la velocidad de conexión variará según el entorno de red.

Anexo A: Glosario

IP Address

La “IP address” (dirección IP) es la dirección IP interna del router. Para acceder a la interfaz de configuración avanzada, escriba esta dirección IP en la barra de dirección de su buscador. Esta dirección puede ser modificada si es necesario. Para modificar la dirección IP, introduzca la nueva dirección IP y haga clic en “Apply Changes” (Aplicar cambios). La dirección IP que elija debería ser una IP no enrutable. Ejemplos de IP no enrutable son:

192.168.x.x (donde x es una cifra entre el 0 y el 255)

10.x.x.x (en donde x es una cifra entre el 0 y el 255)

Subnet Mask

Algunas redes son demasiado grandes como para permitir que el tráfico de datos se extienda por toda la red. Estas redes se dividen en secciones más pequeñas, más sencillas de gestionar, que se denominan subredes. La máscara de subred está compuesta por la dirección de red y por información reservada para identificar la “subred”.

DNS

DNS es un acrónimo de Domain Name Server (Servidor de nombres de dominio). Un Domain Name Server es un servidor ubicado en Internet que convierte los URL (“Universal Resource Links”, Vínculos de recursos universales) como, por ejemplo, www.belkin.com en direcciones IP. Muchos ISPs no precisan que usted introduzca esta información en el router. Si está utilizando un tipo de conexión de IP estática, es posible que deba introducir una dirección DNS específica y una dirección DNS secundaria para que su conexión funcione correctamente. Si su tipo de conexión es dinámica o PPPoE, es probable que no sea necesario introducir ninguna dirección DNS.

PPPoE

La mayoría de proveedores de ADSL emplean PPPoE como tipo de conexión. Si usted emplea un módem ADSL para conectarse a Internet, es posible que su ISP emplee el PPPoE para introducirle en el servicio.

Su tipo de conexión es PPPoE si:

1. Su ISP le proporcionó un nombre de usuario y contraseña que son necesarios para conectarse a Internet.
2. Su ISP le proporcionó software como WinPOET o Enternet300 que usted emplea para conectarse a Internet
3. Usted debe hacer doble clic en un icono de escritorio distinto del de su navegador para acceder a Internet

   Para configurar el router de forma que utilice PPPoE, introduzca su nombre de usuario y contraseña en los espacios previstos. Una vez introducida la información, haga clic sobre “Apply Changes” (Aplicar cambios).

Una vez aplicados los cambios, el indicador el estado de Internet mostrará el mensaje “connection OK” (Conexión en buen estado) si su router ha sido configurado correctamente.

PPPoA

Introduzca la información de PPPoA en el espacio proporcionado y haga clic en “Next” (Siguiente). Haga clic en “Apply” (Aplicar) para activar los ajustes.

1. Nombre de usuario: introduzca el nombre de usuario. (Suministrado por su ISP).
2. Contraseña: introduzca su contraseña. (Suministrado por su ISP).
3. Confirmación de la contraseña: vuelva a ingresar la contraseña. (Suministrado por su ISP).

4. VPI/VCI - Introduzca aquí los parámetros de su identificador de ruta virtual (VPI) y del identificador de cicuito virtual (VCI). (Suministrado por su ISP).

Desconectar después de X...

La propiedad de desconectar se emplea para desconectar automáticamente el router de su ISP cuando no existe actividad durante un periodo determinado de tiempo. Por ejemplo, al colocar una marca junto a esta opción e introducir “5” en el campo para los minutos, el router se desconectará de Internet después de cinco minutos de falta de actividad en Internet. Esta opción debería ser utilizada si paga su servicio de Internet por minutos.

Canal y SSID

Para modificar el canal de funcionamiento del router, seleccione el canal deseado del menú desplegable y seleccione su canal. Haga clic en “Apply Changes” (Aplicar cambios) para guardar los ajustes. También puede cambiar el SSID. El SSID es el equivalente al nombre de la red inalámbrica. Puede llamar al SSID como desee. Si existen otras redes inalámbricas en su zona, deberá dar a su red inalámbrica un nombre exclusivo. Haga clic dentro del cuadro SSID y escriba un nombre nuevo. Haga clic en “Apply Changes” (Aplicar cambios) para efectuar el cambio.

Emisión de ESSID

Muchos adaptadores inalámbricos de red actuales que están disponibles en el mercado cuentan con una función de inspección de la ubicación. Pueden rastrear el entorno en busca de todas las redes disponibles y permitirá al ordenador seleccionar una de las redes localizadas. Esto ocurrirá si el SSID del ordenador tiene el ajuste “ANY” (Cualquier SSID). Su router de Belkin es capaz de bloquear esta búsqueda aleatoria de una red. Si desactiva la función “ESSID Broadcast” (Emitir ESSID), la única forma de que su ordenador se conecte con la red es estableciendo para el SSID del ordenador el nombre específico de la red (como WLAN). Asegúrese de conocer su SSID (nombre de red) antes de activar esta propiedad. Es posible lograr que su red inalámbrica sea prácticamente invisible. Al desactivar la difusión del SSID, su red no aparecerá en ningún estudio del sitio. Desactivar la emisión del SSID contribuirá a elevar la seguridad.

Encriptación

El empleo de la encriptación puede contribuir a mantener su red segura. El router emplea los modos de encriptación WEP y de acceso protegido Wi-Fi (WPA) para proteger sus datos y dispone de dos tipos de encriptación. 64 bits y 128 bits. La encriptación funciona con un sistema de claves. La clave del ordenador debe coincidir con la clave del router. Hay dos formas de crear una clave. La manera

más sencilla es que el software del router convierta una contraseña que usted ha ingresado en una clave. El método avanzado consiste en introducir las claves manualmente.

Servidores virtuales

Esta función le permitirá enrutar llamadas externas (Internet) para servicios como servidor web (puerto 80), servidor FTP (puerto 21) y otras aplicaciones a través de su router hasta su red interna. Gracias a que sus ordenadores internos están protegidos por un firewall, las máquinas fuera de su red (a través de Internet) no pueden acceder a ellos, ya que no pueden ser 'vistos'. Si necesita configurar el servidor virtual para una aplicación específica, será preciso que se ponga en contacto con el fabricante de la aplicación para descubrir los ajustes de los puertos precisos.

Para introducir las configuraciones de forma manual, introduzca la dirección IP en el espacio provisto para la máquina interna (servidor) y el puerto o los puertos necesarios para pasar, seleccione el tipo de puerto (TCP o UDP) y los puertos LAN y públicos necesarios para pasar. Luego, seleccione "Enable" y haga clic en "Set". Sólo puede pasar un puerto por cada dirección IP interna. Abrir puertos en su firewall puede significar un riesgo para la seguridad de la red. Puede activar y desactivar los ajustes con gran rapidez. Se recomienda desactivar las configuraciones cuando no esté utilizando una aplicación específica.

Filtros para IP de clientes

El router puede ser configurado para restringir el acceso a Internet, al e-mail o a otros servicios de red en determinados días y horas. Puede establecerse una restricción para un ordenador, un rango de ordenadores o múltiples ordenadores.

Filtrado de direcciones MAC

El filtro de direcciones MAC es una potente característica de seguridad que le permite especificar qué ordenadores están permitidos en la red. Cualquier ordenador que trate de acceder a la red y no esté especificado en la lista de filtrado no obtendrá permiso para acceder. Cuando active esta propiedad, deberá introducir un nombre de usuario y la dirección MAC de cada cliente de su red para permitir el acceso a la misma de cada uno de ellos o copiar la dirección MAC seleccionando el nombre del ordenador en la lista "DHCP Client List". Para activar esta función, seleccione "Enable". Haga clic en "Apply Changes" (Aplicar cambios) para guardar los ajustes.

DMZ

Si uno de los clientes conectados no puede llevar a cabo una aplicación de Internet correctamente debido al firewall, podrá establecer un acceso a Internet no restringido en ambas direcciones para dicho ordenador. Esto puede ser necesario en el caso de que la propiedad NAT esté causando problemas con una aplicación como, por ejemplo, una aplicación de juegos o de videoconferencia. Utilice esta característica de forma temporal. **El ordenador que se encuentra en la DMZ no está protegido contra los ataques de piratas informáticos.** Para establecer una zona desmilitarizada para uno de los ordenadores, introduzca los últimos dígitos de la dirección IP de LAN en el campo “Static IP” (IP estática) y haga clic en “Apply Changes” (Aplicar cambios) para activar los ajustes.

Si sólo tiene una dirección IP (WAN) pública, deje como IP pública “0.0.0.0”. Si está utilizando múltiples direcciones IP públicas de WAN, será posible seleccionar a qué dirección IP de WAN será dirigido el host de DMZ. Introduzca la dirección IP de WAN a la que desee dirigir el host de DMZ, introduzca los dos últimos dígitos de la dirección IP del ordenador host de DMZ y haga clic en “Apply Changes” (Aplicar cambios).

Contraseña de administrador

El router efectúa el envío SIN necesidad de introducir contraseña. Si desea añadir una contraseña para disfrutar de una mayor seguridad, puede establecerla desde la interfaz de internet del router. Escriba su contraseña y guárdela en un lugar seguro, ya que la necesitará si precisa acceder al router en el futuro. Se **recomienda encarecidamente** que establezca una contraseña si prevé utilizar la opción de gestión a distancia de su router. La opción de tiempo límite de acceso le permite establecer el periodo de tiempo que podrá permanecer en la interfaz de configuración avanzada del router. El temporizador se inicia cuando deja de detectarse actividad. Por ejemplo, usted ha efectuado algunos cambios en la interfaz de configuración avanzada y después deja su ordenador solo sin hacer clic en “Logout” (Salir).

Si suponemos que el tiempo límite es de 10 minutos, entonces 10 minutos después de que abandone el ordenador, la sesión se cerrará. Deberá acceder al router de nuevo para realizar más cambios. La opción del tiempo límite de acceso responde a razones de seguridad y el tiempo predeterminado es de 10 minutos. Solamente podrá acceder un ordenador cada vez a la interfaz de configuración avanzada del router.

Hora y Zona horaria

El router mantiene la hora conectándose a un servidor SNTP (Simple Network Time Protocol, protocolo horario de red simple). Esto permite al router sincronizar el reloj del sistema con la red global de Internet. El reloj sincronizado en el router se utiliza para grabar el registro de seguridad y controlar el filtro de clientes. Seleccione la zona horaria en la que reside. Si reside en una zona que se realiza el cambio de hora según el horario de verano, coloque una marca en el recuadro junto a “Enable Daylight Saving” (Cambiar la hora autiomáticamente según el horario de verano). Puede que el reloj del sistema no se actualice de forma inmediata. Espere al menos 15 minutos para que el router contacte con los servidores horarios de Internet y obtenga una respuesta.

Gestión a distancia

Antes de activar esta función, **ASEGÚRESE DE HABER ESTABLECIDO LA CONTRASEÑA DEL ADMINISTRADOR**. La gestión a distancia le permite efectuar cambios en los ajustes de su router desde cualquier parte en Internet.

UPnP

El UPnP (Universal Plug-and-Play, Plug-and-Play universal) es una tecnología que ofrece un funcionamiento perfecto de las opciones de mensajes de voz, mensajes de vídeo, juegos y otras aplicaciones compatibles con UPnP. Algunas aplicaciones requieren que el firewall del router sea configurado de una forma específica para funcionar correctamente. Normalmente se requiere abrir los puertos TCP y UDP y en algunos casos establecer puertos de disparo. Una aplicación compatible
con UpnP tiene la capacidad de comunicarse con el router, básicamente “diciendo” al router la forma en que necesita que sea configurado el firewall. El router que se le ha suministrado viene con la función UPnP desactivada. Si está utilizando cualquier aplicación compatible con UPnP y desea sacar partido de las características UPnP, puede activar la característica UPnP. Simplemente deberá seleccionar “Enable” (activar) en la sección “UPnP Enabling” (activación de UPnP) de la página de “Utilities” (utilidades). Haga clic en “Apply Changes” (Aplicar cambios) para guardar el cambio.

Anexo B: Factores importantes de colocación e instalación

Nota: Aunque algunos de los artículos enumerados a continuación pueden afectar el rendimiento de la red, estos no impedirán que su red inalámbrica funcione. Si le preocupa que su red no esté funcionando con la máxima eficacia, esta lista de verificación puede ser útil.

1. **Colocación del router inalámbrico**

   Coloque su router inalámbrico (o punto de acceso), el punto central de conexión de su red, lo más cerca posible del centro de sus dispositivos de interconexión en red inalámbricos.

Para lograr la mejor cobertura de red inalámbrica para sus “clientes inalámbricos” (es decir, ordenadores equipados con tarjetas de red inalámbrica para ordenador portátil, tarjetas de red inalámbrica para ordenador de sobremesa y adaptadores inalámbricos para USB de Belkin):

- Asegúrese de que las antenas de red de su router inalámbrico (o punto de acceso) estén situadas de forma paralela entre sí y orientadas verticalmente (apuntando hacia el techo). Si su router inalámbrico (o punto de acceso) está colocado en posición vertical, oriente las antenas hacia arriba en la máxima medida posible.
- En las casas de varias plantas, coloque el router inalámbrico (o punto de acceso) sobre el suelo más cercano posible al centro de la casa. Esto puede implicar la colocación del router inalámbrico (o punto de acceso) en uno de los pisos superiores.
- Intente no colocar el router inalámbrico (o punto de acceso) cerca de un teléfono inalámbrico de 2,4 GHz.

2. **Evitar obstáculos e interferencias**

   Evite colocar su router inalámbrico o punto de acceso cerca de dispositivos que puedan emitir “ruido” de radioemisión, como hornos microondas. Los objetos densos que pueden impedir la comunicación inalámbrica incluyen:

   - Frigoríficos
   - Lavadoras y secadoras
   - Armarios metálicos
   - Acuarios de gran tamaño
   - Ventanas con tinte de base metálica contra radiaciones ultravioletas

Si su señal inalámbrica parece debilitarse en algunos puntos, asegúrese de que este tipo de objetos no esté bloqueando la ruta de la señal (entre sus ordenadores y el router inalámbrico o punto de acceso).

3. Telefónos inalámbricos

Si el rendimiento de su red inalámbrica sigue afectado después de tener en cuenta los aspectos mencionados anteriormente, y usted tiene un teléfono inalámbrico:

- Pruebe a alejar los teléfonos inalámbricos de su router inalámbrico (o puntos de acceso) y de sus ordenadores con equipamiento inalámbrico.
- Desconecte y quite la batería de todos los teléfonos inalámbricos que operen dentro de la banda de 2,4GHz (consulte la información del fabricante). Si se solventa el problema de esta forma, su teléfono probablemente esté causando interferencias.
- Si su teléfono permite la selección de canales, modifique el canal del teléfono para situarlo en el canal más alejado de su red inalámbrica. Por ejemplo, sitúe el teléfono en el canal 1 y su router inalámbrico (o punto de acceso) en el canal 11. Consulte el manual del usuario de su teléfono para obtener instrucciones detalladas.
- En caso necesario, considere la posibilidad de cambiar su teléfono inalámbrico por uno de 900MHz o 5GHz.

4. Seleccionar el canal “más tranquilo” para su red inalámbrica

En lugares en los hay viviendas y oficinas cercanas, como por ejemplo, edificios de apartamentos o complejos de oficinas, es posible que existan redes inalámbricas en los alrededores que puedan entrar en conflicto con la suya.

Emplee la capacidad de inspección de la ubicación de la Utilidad de LAN inalámbrica de su adaptador inalámbrico para localizar otras redes inalámbricas disponibles (véase el manual del adaptador inalámbrico), y coloque su router inalámbrico (o punto de acceso) y ordenadores en un canal lo más alejado posible del resto de redes.

Pruebe con más de uno de los canales disponibles con el fin de descubrir la conexión más nítida y de evitar las interferencias de teléfonos inalámbricos cercanos o de otros dispositivos inalámbricos.

Para los productos de interconexión en red inalámbrica de Belkin, utilice la información detallada de Inspección de la ubicación y de canales inalámbricos incluida en su Guía del Usuario

Estas directrices deberán permitirle abarcar la zona más extensa posible con su router inalámbrico (o punto de acceso). En caso de que necesite abarcar un área más amplia, le recomendamos el Módulo de Extensión de Alcance Inalámbrico/Punto de Acceso de Belkin.

5. Conexiones seguras, VPN y AOL

Las conexiones seguras requieren normalmente un nombre de usuario y una contraseña y se utilizan cuando la seguridad es importante. Las conexiones seguras incluyen:

- Conexiones de red virtual privada (VPN), utilizadas con frecuencia para conectar a distancia con una red de oficina
- El programa “Bring Your Own Access” (trae tu propio acceso) de America Online (AOL), que le permite emplear AOL a través de la banda ancha proporcionada por otro servicio por cable o DSL
- La mayoría de las páginas-web de servicios bancarios online
- Muchas páginas-web comerciales requieren un nombre de usuario y una contraseña para acceder a su cuenta

Las conexiones seguras pueden verse interrumpidas por una configuración de gestión de la alimentación del ordenador que le haga pasar al modo de ahorro de energía. La solución más sencilla para evitarlo es conectar de nuevo ejecutando otra vez el software de VPN o AOL, o accediendo de nuevo al sitio web seguro.

Una segunda alternativa consiste en modificar las configuraciones de gestión de la alimentación de su ordenador, de forma que no pase al modo de suspensión; no obstante, esto puede no ser apropiado para ordenadores portátiles. Para modificar su configuración de gestión de la alimentación en Windows, consulte las “Opciones de Alimentación” en el Panel de Control.

Si continúa teniendo dificultades con la conexiones seguras, VPNs y AOL, revise los pasos descritos en las páginas anteriores para asegurarse de haber tratado estos temas.

Anexo C: Tabla de ajustes para la conexión a Internet

La tabla a continuación le proporciona una referencia para le selección y configuración de la conexión de Internet de ADSL. Muchos ISPs utilizan ajustes diferentes según la región y el equipo utilizado. Intente los ajustes para los ISPs en su región. Si éstos no funcionan, póngase en contacto con su ISP para obtener sus ajustes exactos.

País	Protocolo de conexión	VPI/VCI	Encapsulamiento	ISPs
Europa				
Francia	PPPoE	8/35	LLC	Varios
Germany	PPPoE	1/32	LLC	T-Online, varios
Países Bajos	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Varios
Bélgica	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italia	PPPoE o PPPoA	8/35	VC MUX	TIN
España	PPPoE o 1483 Bridged	8/32	LLC	Telefonica
Suecia	1483 Bridged	3/35	LLC	Telia
UK	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Asia				
Australia	PPPoE o PPPoA	8/35	LLC	Varios
Nueva Zelanda	PPPoE o PPPoA	0/100	VC MUX	Varios
Singapur	PPPoE	0/100	LLC	SingNet, Pacific Internet

Declaración de la FCC

DECLARACIÓN DE CONFORMIDAD CON LAS NORMATIVAS DE LA FCC SOBRE COMPATIBILIDAD ELECTROMAGNÉTICA

Nosotros, Belkin Corporation, con sede en 501 West Walnut Street, Compton, CA 90220, EE.UU., declaramos bajo nuestra sola responsabilidad que el producto

F5D9630-4

al que hace referencia la presente declaración, cumple con la sección 15 de las normativas de la FCC. Su utilización está sujeta a las siguientes dos condiciones: (1) este dispositivo no debe provocar interferencias nocivas y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan provocar un funcionamiento no deseado.

Advertencia: Exposición a las radiaciones de radiofrecuencia.

La energía de salida emitida por este dispositivo se encuentra muy por debajo de los límites de exposición a radiofrecuencias de la FCC. No obstante, el dispositivo será empleado de tal forma que se minimice la posibilidad de contacto humano durante el funcionamiento normal.

Cuando se conecta una antena externa al dispositivo, dicha antena deberá ser colocada de tal manera que se minimice la posibilidad de contacto humano durante el funcionamiento normal. Con el fin de evitar la posibilidad de superar los límites de exposición a radiofrecuencias establecidos por la FCC, la proximidad del ser humano a la antena no deberá ser inferior a los 20 cm (8 pulgadas) durante el funcionamiento normal.

Declaración de la Federal Communications Commission (FCC, Comisión de comunicaciones de EE.UU.)

Las pruebas realizadas con este equipo dan como resultado el cumplimiento con los límites establecidos para un dispositivo digital de la Clase B, de acuerdo a la Sección 15 de las Normas de la FCC. Estos límites se han establecido con el fin de proporcionar una protección suficiente contra interferencias nocivas en zonas residenciales.

Este equipo genera, emplea y puede irradiar energía de radiofrecuencia. Si este equipo provoca interferencias nocivas en la recepción de radio y televisión, las cuales se pueden determinar encendiendo y apagando seguidamente el dispositivo, el mismo usuario puede intentar corregir dichas interferencias tomando una o más de las siguientes medidas:

- Reorientar o colocar en otro lugar la antena de recepción.
- Aumentar la distancia entre el equipo y el receptor.
- Conectar el equipo a la toma de un circuito distinto de aquel al que está conectado el receptor.
- Solicitar la ayuda del vendedor o de un técnico experto en radio/televisión.

Modificaciones
El FCC exige que el usuario sea notificado de que cualquier cambio o modificación del presente dispositivo que no sea aprobado expresamente por Belkin Corporation podría invalidar el derecho del usuario para utilizar este equipo.

Canadá: Industry Canada (IC)
La radioemisión inalámbrica de este dispositivo cumple las especificaciones RSS 139 y RSS 210 de Industry Canada. Este aparato digital de la Clase B cumple con la norma canadiense ICES-003.

Este dispositivo digital de la Clase B cumple la norma canadiense NMB-003.

Europa: Declaración de la Unión Europea

CE 0560 ⓘ

Los productos de radioemisión con la indicación CE 0560 o CE cumplen con la Directiva R&TTE (1995/5/CE) de la Comisión, de las Comunidades Europeas.

El cumplimiento de esta directiva implica la conformidad con las siguientes Normas Europeas (entre paréntesis se encuentran las normativas internacionales equivalentes).

CE ⓘ

- EN 60950 (IEC60950) – Seguridad de los productos
- EN 300 328 Requisitos técnicos para equipos de radioemisión
- ETS 300 826 Requisitos generales de la EMC para equipos de radioemisión.

Para determinar el tipo de transmisor, compruebe la etiqueta de identificación de su producto Belkin.

Los productos con la indicación CE cumplen con la directiva EMC (89/336/CEE) y la Directiva de Bajo Voltaje (72/23/CEE) establecidas por la Comisión de las Comunidades Europeas. El cumplimiento de estas directivas implica la conformidad con las siguientes Normas Europeas (entre paréntesis se encuentran las normativas internacionales equivalentes).

CE

- EN 55022 (CISPR 22) – Interferencias electromagnéticas
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Inmunidad electromagnética
- EN 61000-3-2 (IEC610000-3-2) – Movimiento armónico de la línea eléctrica
- EN 61000-3-3 (IEC610000) – Fluctuaciones de la línea eléctrica
- EN 60950 (IEC60950) – Seguridad de los productos

Los productos que contienen el radiotransmisor llevan la etiqueta CE 0560 o CE y es posible que lleven asimismo el logotipo CE.

Este símbolo en el producto o su embalaje indica que este producto no debe desecharse junto con la basura. En lugar de ello, es responsabilidad suya entregar el equipamiento que quiere desechar en un punto de recogida para el reciclaje de electrodomésticos y equipamiento electrónico. La recogida selectiva y el reciclado del equipo que desea desechar ayudará a conservar los recursos naturales y a asegurar que se recicla de manera que no perjudique la salud humana ni el medio ambiente. Para más información sobre dónde puede entregar el equipo para su reciclado, póngase en contacto con el ayuntamiento de su localidad, el servicio de recogida de basuras o el establecimiento donde adquirió el producto.



Garantía de por vida del producto de Belkin Corporation Limited

Belkin Corporation proporciona para el presente producto una garantía para toda la vida de reparación gratuita, por lo que respecta a mano de obra y materiales. En el caso de presentarse un fallo, Belkin decidirá entre la reparación del mismo o la sustitución del producto, en ambos casos sin costes, siempre que se devuelva durante el periodo de garantía y con los gastos de transporte abonados al vendedor autorizado de Belkin en el que se adquirió. Es posible que se solicite una prueba de compra.

Esta garantía perderá su validez en el caso de que el producto haya sido dañado de forma accidental, por abuso o utilización errónea del mismo; si el producto ha sido modificado sin la autorización por escrito de Belkin; o si alguno de los números de serie de Belkin ha sido eliminado o deteriorado.

LA GARANTÍA Y RESTITUCIONES LEGALES ESTABLECIDAS EXPRESAMENTE EN EL PRESENTE ACUERDO SUSTITUYEN A TODAS LAS DEMÁS, ORALES O ESCRITAS, EXPRESAS O IMPLÍCITAS. BELKIN RECHAZA DE MANERA EXPLÍCITA TODAS LAS DEMÁS GARANTÍAS IMPLÍCITAS, INCLUYENDO, SIN LIMITACIÓN, LAS GARANTÍAS DE COMERCIABILIDAD Y DE IDONEIDAD PARA UN FIN ESPECÍFICO.

Ningún distribuidor, agente o empleado de Belkin está autorizado a realizar ningún tipo de modificación, extensión o alteración de la presente garantía.

BELKIN NO SE HARÁ EN NINGÚN CASO RESPONSABLE POR LOS DAÑOS IMPREVISTOS O RESULTANTES DE UN INCUMPLIMIENTO DE LA GARANTÍA, O BAJO NINGUNA OTRA CONDICIÓN LEGAL, INCLUYENDO, PERO NO EXCLUSIVAMENTE, LOS BENEFICIOS PERDIDOS, PERIODOS DE INACTIVIDAD, BUENA VOLUNTAD, DAÑOS DURANTE LA REPROGRAMACIÓN O REPRODUCCIÓN DE CUALQUIERA DE LOS PROGRAMAS O DATOS ALMACENADOS EN O EMPLEADOS CON LOS PRODUCTOS BELKIN.

Algunas jurisdicciones no permiten la exclusión o limitación de los daños imprevistos o consecuentes ni las exclusiones de las garantías implícitas, por lo que cabe la posibilidad de que las anteriores limitaciones o exclusiones no le afecten. Esta garantía le proporciona derechos legales específicos y usted puede beneficiarse asimismo de otros derechos legales específicos que varían entre las distintas jurisdicciones.

Módem ADSL2+ con router inalámbrico G+ MIMO

Podrá encontrar más información en nuestra página web, www.belkin.com, a través del servicio de asistencia técnica.
“Si desea ponerse en contacto con el servicio de asistencia técnica por teléfono, le rogamos que llame al número correspondiente de la siguiente lista*. La asistencia técnica está a su disposición 24 horas al día, 7 días a la semana.”

*Pueden aplicarse tarifas de llamada nacional

Asistencia técnica gratuita*

AUSTRIA	08 - 20 20 07 66	LUXEMBURGO	34 20 80 8560
REPÚBLICA CHECA	23 900 04 06	PAÍSES BAJOS	0900 - 040 07 90
DINAMARCA	701 22 403	NORUEGA	815 00 287
FINLANDIA	00800 - 22 35 54 60	POLONIA	00800 - 441 17 37
FRANCIA	08 - 25 54 00 26	PORTUGAL	707 200 676
ALEMANIA	0180 - 500 57 09	RUSIA	495 580 9541
GRECIA	00800 - 44 14 23 90	SUDÁFRICA	0800 - 99 15 21
HUNGRÍA	06 - 17 77 49 06	ESPAÑA	902 - 02 43 66
ISLANDIA	800 8534	SUECIA	07 - 71 40 04 53
IRLANDA	0818 55 50 06	SUIZA	08 - 48 00 02 19
ITALIA	02 - 69 43 02 51	REINO UNIDO	0845 - 607 77 87

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Ángeles, CA 90220-5221, EE.UU.
310-898-1100
310-898-1111 fax

Belkin Ltd.
7 Bowen Crescent, West Gosford
NSW 2250, Australia
+61 (0) 2 4372 8600
+61 (0) 2 4372 8603 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Reino Unido
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Abnegué 333
1119 PH Schiphol-Rijk, Países Bajos
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

P75125ea_A

BELKIN

Modem ADSL2+ con router G+ MIMO wireless

Per collegare in rete diversi computer e condividere l'accesso a Internet in ADSL

UK
FR
DE
NL
ES
IT



Manuale d'uso

802.11g
G+
MIMO

F5D9630it4A

Indice

Grazie per aver scelto il Modem ADSL con Router Wireless G High-Speed Mode Belkin (il router). Con questo nuovo router sarà possibile condividere in pochi minuti la stessa connessione a Internet e collegare in rete diversi computer. Di seguito è riportato un elenco delle caratteristiche che fanno di questo nuovo router una soluzione ideale per la creazione di una rete in casa o in un piccolo ufficio. Vi invitiamo a leggere con attenzione questo manuale, in particolare l'Allegato B intitolato "Considerazioni importanti per il posizionamento e la configurazione".

I vantaggi di una rete domestica

Seguendo le nostre semplici istruzioni di configurazione è possibile utilizzare la propria rete domestica Belkin pe r:

- condividere la connessione ad alta velocità a Internet con tutti i computer di casa;
- condividere risorse, quali file e dischi rigidi, tra tutti i computer collegati alla rete domestica;
- Condividere una sola stampante tra tutta la famiglia;
- Condividere documenti, musica, video e fotografie digitali;
- Memorizzare, recuperare e copiare file da un computer all'altro;
- Disputare partite online, controllare la posta elettronica e chattare da diversi computer contemporaneamente.

I vantaggi di una rete wireless Belkin

Mobilità - la "stanza per il computer" non è più necessaria: da oggi si può lavorare da un portatile o da un computer desktop collegato in rete da un qualsiasi punto all'interno della propria copertura wireless

Facilità di installazione - il programma di installazione guidata Belkin facilita la procedura di configurazione

Versatilità - si ha la possibilità di accedere a stampanti, computer e altri dispositivi di rete da qualsiasi punto all'interno della propria abitazione

Facilità di espansione - la vasta gamma dei prodotti di rete Belkin permette di espandere la propria rete, aggiungendo altri dispositivi tra i quali stampanti e console di gioco

Niente cavi - non è più necessario spendere soldi e perdere tempo per cablare la propria abitazione o l'ufficio per creare una connessione Ethernet

Accettazione incondizionata di altre marche - si ha la possibilità di scegliere tra una vasta gamma di prodotti di rete interoperabili

Materiale necessario

Contenuto della confezione

- Modem ADSL2+ con Router G+ MIMO Wireless
- Cavo telefonico RJ11 - Grigio
- Cavo di rete RJ45 Ethernet - Giallo
- Microfiltro ADSL*
- Adattatore di corrente
- Manuale d'uso

*il microfiltro ADSL varia di paese in paese. Se non fosse compreso nella fornitura, sarà necessario acquistarne uno.

Requisiti del sistema

- Un servizio ADSL attivo con una presa telefonica a muro per collegare il router
- Almeno un computer con una scheda di interfaccia di rete (NIC) e un browser web installato e configurato correttamente
- Protocollo di rete TCP/IP installato su ogni computer e collegato al router
- Nessun altro server DHCP sulla propria rete locale che assegni gli indirizzi IP ai computer e agli altri dispositivi

Impostazionidi connessione a Internet

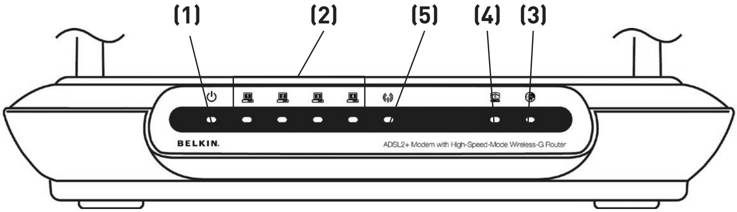
Prima di configurare il router G wireless con modem ADSL è necessario richiedere le seguenti informazioni al proprio ISP.

- Protocollo di connessione a Internet: ________ (PPPoE, PPPoA, IP dinamico, IP statico)
- Metodo Multiplexing o incapsulamento: __________ (LLC oppure VC MUX)
- Circuito virtuale: VPI (Virtual Path Identifier) __________ (un numero compreso tra 0 e 255)
- VCI (Virtual Channel Identifier) __________ (un numero compreso tra 1 e 65535)
- Per utenti PPPoE e PPPoA: nome utente _____________ e password ______________ dell'account ADSL
- Per gli utenti IP statici: Indirizzo IP ___ . ___ . ___ . ___
  Maschera di sottorete ___ . ___ . ___ . ___
  Server Gateway predefinito ___ . ___ . ___ .
- Indirizzo IP del Domain Name Server ___ . ___ . ___ . ___ (se assegnato dal proprio ISP)

Nota bene: per conoscere alcuni dei parametri di impostazione Internet DSL comuni, vedere l'Appendice C di questo manuale. Nel dubbio, contattare il proprio ISP.

Il router è stato progettato per essere posizionato su una scrivania. Tutti i cavi escono dal retro del router, consentendo una migliore organizzazione e utilizzabilità. Gli indicatori LED sono facilmente visibili sulla parte anteriore del router e mantengono informati sull'attività e sullo stato della rete.

Pannello anteriore



1. LED alimentazione

L'accensione o il riavvio del router richiedono un breve intervallo di attesa. Una volta riavviato completamente il router, nel LED che segnala lo stato di alimentazione si accende una spia VERDE, che sta ad indicare che il router è pronto all'uso.

	OFF	Il router NON è attivo
	Verde	Il router è ATTIVO
	Rosso	Il router non si è attivato

2. LED di stato LAN

Questi LED di indicazione dello stato LAN sono contrassegnati con i numeri da 1 a 4 e corrispondono alle porte numerate previste sul retro del router. Quando un computer viene collegato correttamente ad una delle porte LAN sul retro del router, si accendono i LED. Una spia VERDE fissa indica la presenza di un computer o di un dispositivo di rete collegato. Quando l'informazione viene trasmessa attraverso la porta, il LED lampeggia rapidamente. La spia ARANCIONE indica la presenza di una connessione 10Base-T.

	OFF	Nessun dispositivo collegato
	Arancione	Il collegamento alla rete Ethernet è attivo e il dispositivo 10Base-T è collegato
	Arancione - Lampeggiante	Il dispositivo 10Base-T sta ricevendo o trasmettendo i dati
	Verde	Il collegamento alla rete Ethernet è attivo e il dispositivo 100Base-T è collegato
	Verde - Lampeggiante	Il dispositivo 100Base-T sta ricevendo o trasmettendo i dati

3. **LED di segnalazione stato WLAN**

Nel LED di segnalazione stato WLAN quando la funzione LAN wireless viene attivata si accende una spia VERDE fissa. Se lampeggia, significa che il router sta trasmettendo o ricevendo i dati in modalità wireless.

	OFF	WLAN è disattivata
	Verde	La connessione WLAN è attiva
	Verde - Lampeggiante	Durante la trasmissione o la ricezione dei dati

4. **LED ADSL**

Nel LED ADSL, durante la fase di negoziazione con l'ISP, si accende una spia VERDE lampeggiante. Rimane VERDE una volta che il router è correttamente collegato al proprio servizio ADSL.

	OFF	Nessuna connessione ADSL
	Verde	Collegamento ADSL attivo
	Verde - lampeggiante	negoziazione della connessione

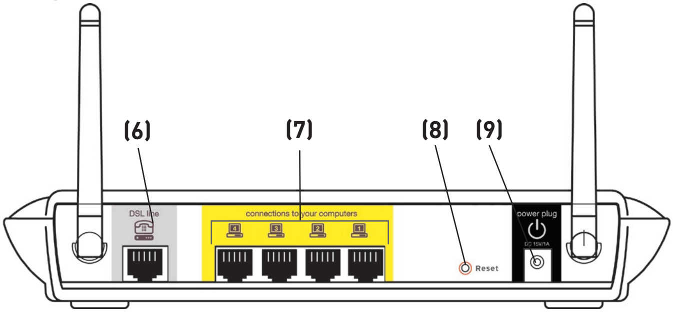
5. **LED Internet**

Il LED Internet segnala quando il router è collegato a Internet. Se il LED è SPENTO, significa che il router NON è collegato ad Internet. Se il LED è VERDE e acceso in maniera fissa, significa che il router è collegato ad Internet. Se il LED lampeggia, significa che il router sta trasmettendo o ricevendo dati da Internet.

	OFF	Nessuna connessione a Internet
	Verde	Connesso a Internet
	Verde - lampeggiante	Durante la trasmissione o la ricezione dei dati
	Rosso	Mancata ricezione dell'IP

sezione
1
2
3
4
5
6
7
8
9
10

Pannello posteriore



6. **Linea DSL**
   Questa porta consente di impostare il collegamento con la propria linea ADSL. La linea ADSL deve essere collegata a questa porta.

7. **Porte Ethernet**
   Le porte Ethernet sono RJ45, 10/100 auto-negoziazione. Queste porte sono contrassegnate con i numeri da 1 a 4 e corrispondono ai LED numerati presenti sulla parte anteriore del router. I propri computer abilitati alla connessione in rete e tutti gli altri dispositivi di rete vanno collegati ad una di queste porte.

8. **Pulsante di Reset**
   Il pulsante di Reset viene utilizzato in alcuni casi rari, quando il router non funziona correttamente. Resettando il router, si ripristina la normale modalità di funzionamento del router pur mantenendo le impostazioni programmate. Il pulsante di reset consente anche di ripristinare le impostazioni predefinite. L'opzione di ripristino si può utilizzare ad esempio nel caso sia stata dimenticata la password cliente.

   a. **Reset del router**
      Premere per un secondo il pulsante di Reset, quindi rilasciarlo. Quando la spia alimentazione/pronto è di nuovo fissa, significa che l'operazione di reset è stata completata.

   b. **Ripristino delle impostazioni predefinite**
      Premere e tenere premuto il pulsante di reset per cinque secondi, quindi lasciarlo. Quando la spia alimentazione/pronto è di nuovo fissa, significa che l'operazione di ripristino è stata completata.

9. **Presa di alimentazione**
   Il cavo di alimentazione da 15V CC va collegato a questa presa. L'utilizzo di un tipo di adattatore di alimentazione sbagliato può danneggiare il router.

Collocazione del router

Minore è la distanza tra il computer e il router o l’access point e maggiore è l’intensità della connessione wireless. La copertura tipica per i dispositivi wireless in un ambiente chiuso è compresa tra i 30 e i 60 metri. Analogamente, la qualità della connessione e delle prestazioni wireless sarà leggermente inferiore aumentando la distanza tra i dispositivi collegati al router. Tuttavia, questa condizione potrebbe passare inosservata. All’aumentare della distanza dal router, la velocità della connessione potrebbe diminuire. Apparecchiature in metallo, ostacoli e muri rientrano tra i fattori che indeboliscono i segnali, invadendo il raggio d’azione delle onde radio della rete. Vedere l’”Allegato B: Considerazioni importanti per il posizionamento e la configurazione” in questo Manuale per ulteriori informazioni in merito.

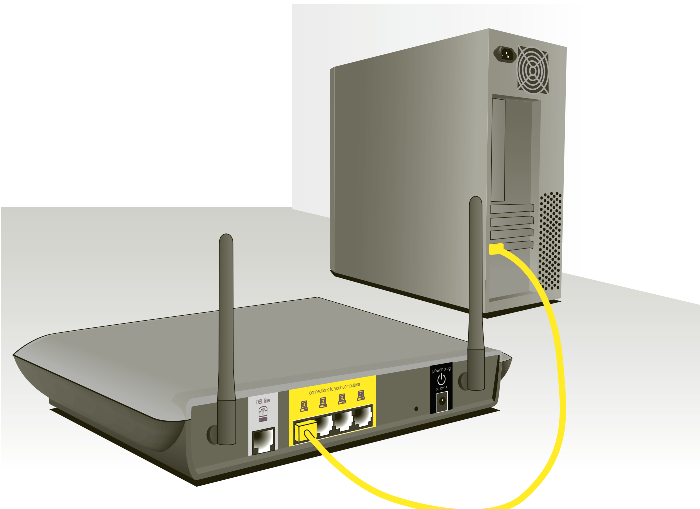
Per verificare se eventuali problemi di prestazione della rete siano dovuti alla presenza di ostacoli nell’area di copertura, provare a posizionare il computer ad una distanza compresa tra 1,5 m e 3 m dal router. Se i problemi persistono anche ad una distanza inferiore, consultare la sezione dedicata alla risoluzione dei problemi.

1
2
3
4
5
6
7
8
9
10
sezione

Collegamento dei computer

1. Spegnere i computer e l'attrezzatura di rete.

2. Collegare il proprio computer ad una delle porte GIALLE RJ45 sul retro del router contrassegnate con "connections to your computers" utilizzando un cavo di rete Ethernet (un cavo di rete Ethernet è fornito).



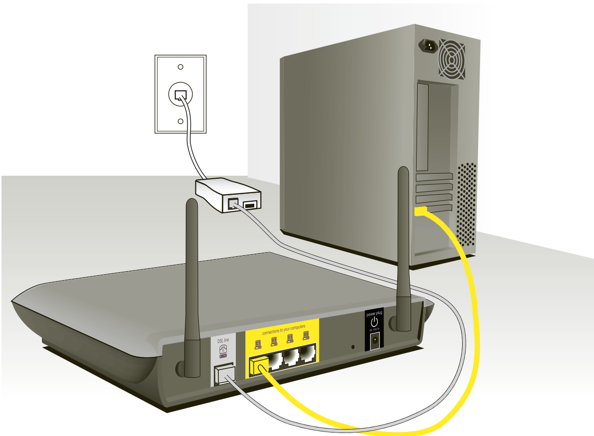
Collegamento della linea ADSL

Il collegamento per il router alla linea ADSL varia in base al Paese e alla regione. Generalmente prevede un microfiltro o un microfiltro con splitter integrato per l'utilizzo contemporaneo del servizio ADSL e del servizio telefonico sulla stessa linea. Leggere con attenzione i seguenti passaggi e scegliere il metodo più adatto.

1. Se il servizio telefonico e il servizio ADSL non sono sulla stessa linea telefonica, sono necessari alcuni microfiltri ADSL per ogni telefono e altro apparecchio, quale la segreteria telefonica, il fax e il display di visualizzazione dell'ID del chiamante. Per separare le linee telefoniche ed il router si possono utilizzare altri splitter supplementari.

   Nota bene:non collegare il microfiltro ADSL tra la presa a muro ed il router, in quanto questo accorgimento impedirebbe al servizio ADSL di raggiungere
   il modem.

2. Se il servizio telefonico e il servizio ADSL non sono sulla stessa linea telefonica e si sta utilizzando un microfiltro ADSL con splitter integrato, collegare lo splitter alla presa a muro del telefono che eroga il servizio ADSL. Quindi, collegare il cavo telefonico dalla porta RJ11 del microfiltro ADSL generalmente contrassegnata con "DSL" alla porta RJ11 grigia contrassegnata con "DSL line" sul retro del router. Collegare il dispositivo telefonico ad un'altra porta dello splitter ADSL generalmente contrassegnata con "Phone". Per aggiungere un altro telefono e dispositivo sulla stessa linea è necessario prevedere un microfiltro ADSL supplementare.



Nota bene: un cavo telefonico RJ11 è compreso nella confezione. Inserendo il connettore RJ11, assicurarsi che la levetta posta sul connettore scatti in posizione per garantire il corretto inserimento.

3. Se si dispone di una linea di servizio telefonico ADSL dedicata con una presa a muro RJ11, è sufficiente collegare un cavo telefonico dalla presa a muro alla portagrigia RJ11 etichettata "DSL line" sul retro del router.

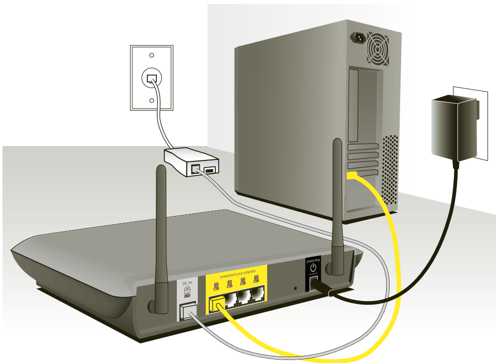
4. Se per il proprio servizio ADSL si dispone di una presa a muro RJ45, collegare un convertitore RJ45-RJ11 alla presa a muro. Quindi collegare un'estremità del cavo telefonico al convertitore e l'altra estremità alla porta grigiaRJ11 etichettata "DSL line" sul retro del router.

Nota bene: il microfiltro ADSL può essere previsto o meno nella fornitura a seconda del Paese di destinazione.

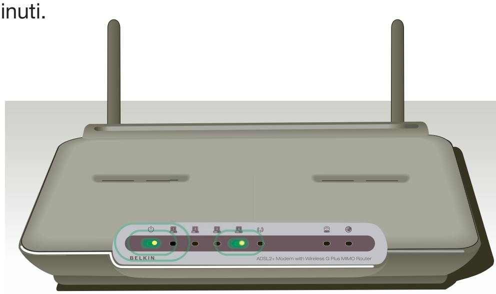
Accensione del router

1. Collegare l'adattatore di alimentazione fornito alla presa di corrente del router etichettata "Power".

   Nota bene:per motivi di protezione e prestazioni, e per evitare danni al router, utilizzare soltanto l'adattatore di alimentazione fornito.



2. Dopo aver collegato l'adattatore di alimentazione ed aver attivato il dispositivo, l'icona di alimentazione del router ⏻ sul pannello anteriore dovrebbe essere attiva. L'avvio completo del router potrebbe richiedere alcuni minuti.



3. Accendere i computer. Dopo aver avviato i computer, si accederà un LED 🖳 di indicazione di stato LAN sulla parte frontale del router per ciascuna porta alla quale è connesso un computer cablato. Queste spie servono ad indicare lo stato di connessione e attività. A questo punto si può procedere con la configurazione del router per eseguire il collegamento ADSL.

Per consentire al computer di comunicare correttamente con il Router, è necessario modificare le impostazioni “TCP/IP Ethernet” e impostarle su “Ottieni automaticamente un indirizzo IP/Utilizza DHCP”. Si tratta dell’impostazione normalmente predefinita nella maggior parte dei computer d’uso domestico.

INNANZITUTTO, impostare il computer collegato al modem ADSL seguendo queste fasi. Le stesse operazioni si possono eseguire anche per aggiungere altri computer al router dopo aver impostato il router in modo da collegarlo ad Internet.

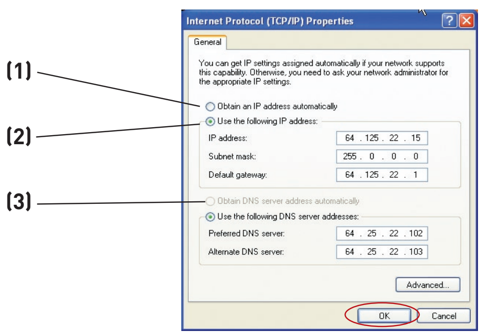
Configurazione manuale degli adattatori di rete in Windows XP, 2000, o NT

1. Fare clic su “Start”, “Impostazioni” e quindi su “Pannello di controllo”.

2. Fare doppio clic sull’icona “Connessioni di rete e accesso remoto” (Windows 2000) o sull’icona “Rete e connessioni Internet (Windows XP).

3. Fare clic con il tasto destro del mouse sull’opzione “Connessione alla rete locale (LAN)” associata alla propria scheda di rete e selezionare “Proprietà” dal menu a tendina.

4. Dalla finestra “Proprietà connessione locale” fare clic su “Protocollo Internet (TCP/IP)”, quindi su “Proprietà”. Compare la seguente schermata.



5. Se l’opzione “Usa il seguente indirizzo IP” **(2)**è selezionata, il router deve essere impostato per un tipo di connessione IP statica. Scrivere le informazioni relative all’indirizzo riportate nella tabella in basso. Queste informazioni devono essere inserite nel router.

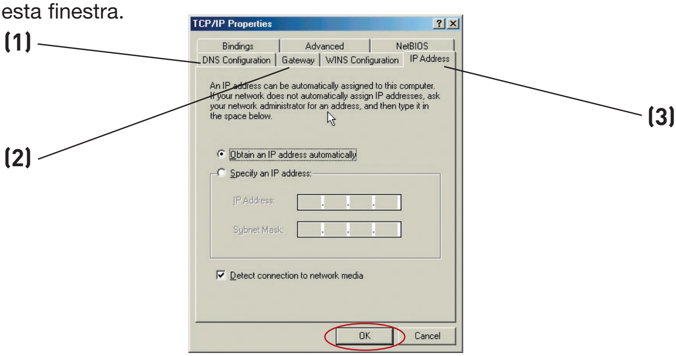
IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

6. Se non fosse già selezionata, selezionare l’opzione “Ottieni automaticamente un indirizzo IP” **(1)** e “Ottieni indirizzo server DNS automaticamente” **(3)**. Fare clic su “OK”.

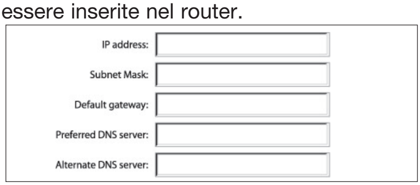
L’adattatore di rete è ora configurato per consentire l’utilizzo del Router.

Configurazione manuale degli adattatori di rete in Windows 98SE o Me

1. Con il tasto destro del mouse, fare clic su "Risorse di rete" e selezionare "Proprietà".
2. Selezionare "Impostazioni TCP/IP" per l'adattatore di rete installato. Si apre questa finestra.



3. Se l'opzione "Specifica l'indirizzo IP" è selezionata, il router deve essere impostato per un tipo di connessione IP statica. Scrivere le informazioni relative all'indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.



4. Compilare i dati per l'indirizzo IP e la scheda di sottorete dalla scheda "Indirizzo IP" **(3)**.
5. Fare clic sulla scheda "Gateway" **(2)**. Trascrivere l'indirizzo gateway nella tabella.
6. Fare clic sulla scheda "Configurazione DNS" **(1)**. Trascrivere l'indirizzo (o gli indirizzi) DNS nella tabella.
7. Se non fosse già selezionata, selezionare l'opzione "Ottieni automaticamente un indirizzo IP" (1) dalla scheda di indirizzo IP. Fare clic su "OK".
8. Per una corretta configurazione di connessione al router Belkin è necessario cancellare l'indirizzo gateway dalla scheda Gateway e i dati di configurazione DNS.

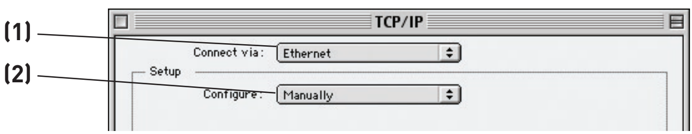
Riavviare il computer. Una volta riavviato il computer, gli adattatori di rete saranno configurati per essere utilizzati con il router.

INNANZITUTTO, impostare il computer collegato al modem via cavo o ADSL seguendo queste fasi. Le medesime operazioni si possono eseguire anche per aggiungere altri computer al router dopo averne impostato il collegamento ad Internet.

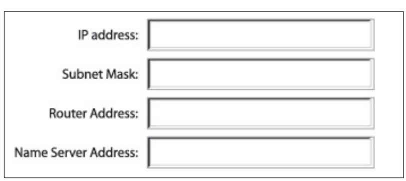
Configurazione manuale delle impostazioni degli adattatori nei sistemi operativi Mac OS fino alla versione 9.x

Per consentire al computer di comunicare correttamente con il router, è necessario modificare le impostazioni TCP/IP del computer Mac in DHCP.

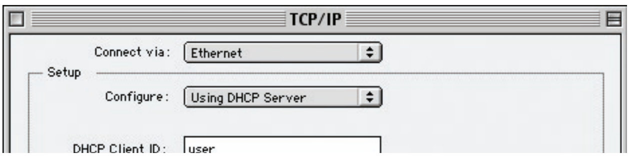
1. Aprire il menu "Apple". Selezionare dapprima "Pannelli di controllo", e quindi "TCP/IP".
2. Compare il pannello di controllo TCP/IP. +Selezionare "Ethernet Built-In" (Ethernet Integrato) o "Ethernet" dal menu a tendina "Connetti tramite". **(1)**.



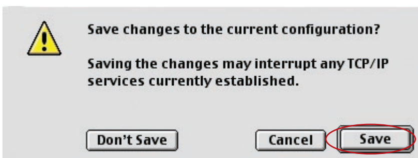
3. Accanto a "Configura" **(2)**, se è stato selezionato "Manualmente", il router deve essere impostato per consentire una connessione IP statica. Scrivere le informazioni relative all'indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.



4. Se non fosse già impostato, nella scheda “Configura”, selezionare “Utilizza server DHCP”. Questo indicherà al computer di ottenere un indirizzo IP dal Router.



5. Chiudere la finestra. Nel caso fossero state fatte alcune modifiche, compare la seguente videata: Fare clic su “Save” (Salva).



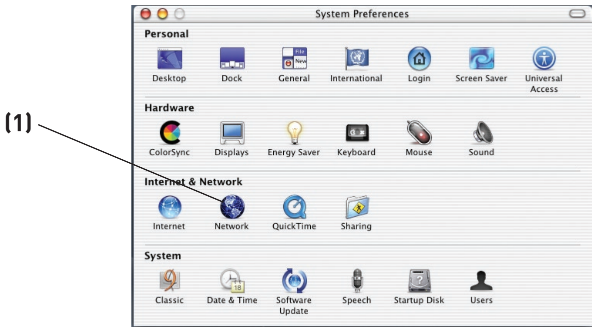
Riavviare il computer. Quando il computer verrà riavviato, le impostazioni di rete saranno configurate per essere utilizzate con il router.

Configurazione manuale degli adattatori di rete nei sistemi operativi Mac

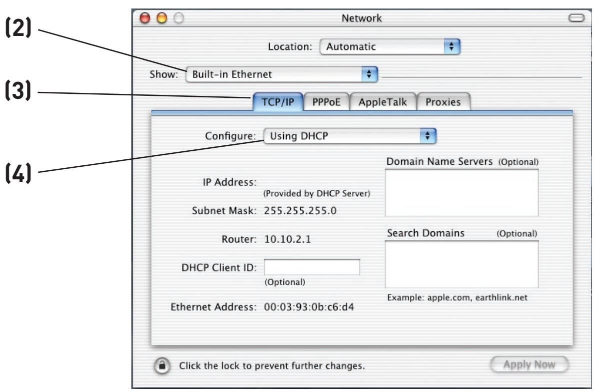
1. Fare clic sull'icona "Preferenze del sistema".



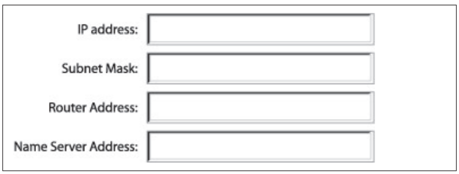
2.Selezionare "Rete" **(1)** dal menu "Preferenze del sistema".



3. Selezionare "Built-in Ethernet" **(2)** accanto all'opzione "Mostra" nel menu "Rete".



4. Selezionare la scheda “TCP/IP” **(3)**. Accanto a “Configura” **(4)**, dovrebbero comparire “Manualmente” o “Utilizza DHCP”. In caso contrario, verificare nella scheda PPPoE **(5)** che l’opzione “Connetti utilizzando PPPoE” NON sia selezionata. Se lo fosse, il router deve essere configurato per un tipo di connessione PPPoE, usando il proprio nome utente e password.
5. Se è stato selezionato “Manualmente”, il router deve essere impostato in modo da eseguire un tipo di connessione IP statico. Scrivere le informazioni relative all’indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.

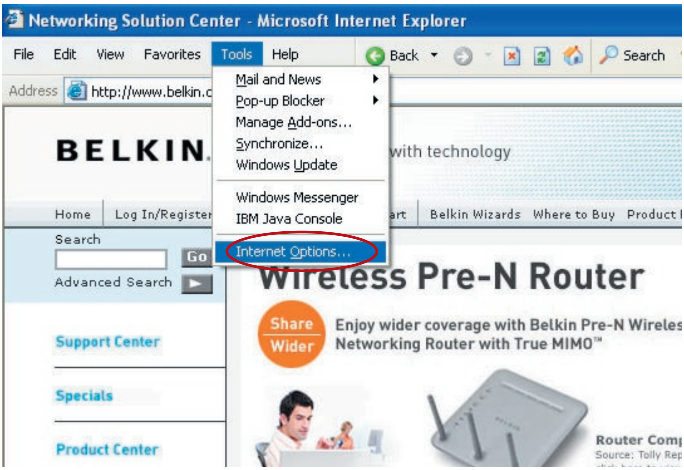


6. Se non fosse già selezionato, selezionare “Utilizza server DHCP” accanto a “Configura” **(4)**, quindi fare clic su “Applica ora”.

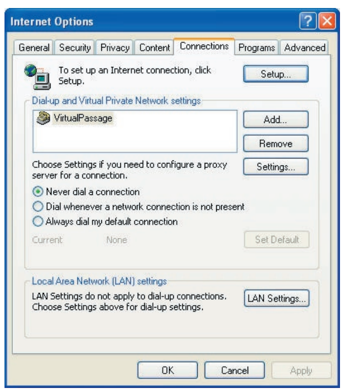
L’adattatore di rete è ora configurato per consentire l’utilizzo del router.

Impostazioni consigliate del browser web

Nella maggior parte dei casi non è necessario eseguire molte modifiche alle impostazioni del browser web. Nel caso l'accesso ad Internet o l'utilizzo dell'interfaccia utente avanzata basata sul web creassero qualche problema, modificare le impostazioni del browser in base alle impostazioni consigliate in questo capitolo.

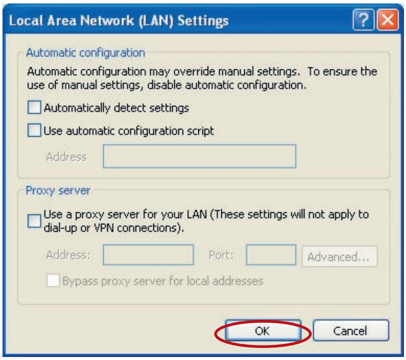


Internet Explorer versione 4.0 o successive



1. Avviare il browser Web. Selezionare "Strumenti" e "Opzioni Internet".
2. Nella schermata "Opzioni Internet" compaiono tre opzioni: "Non utilizzare mai connessioni remote", "Usa connessione remota se non è disponibile una connessione di rete" e "Utilizza sempre la connessione remota predefinita". Se è possibile, selezionare "Non utilizzare mai connessioni remote". Nel caso non fosse possibile eseguire una selezione, passare alla fase successiva.
3. Nella finestra "Opzioni Internet", cliccare su "Connessioni" e selezionare "Impostazioni LAN".

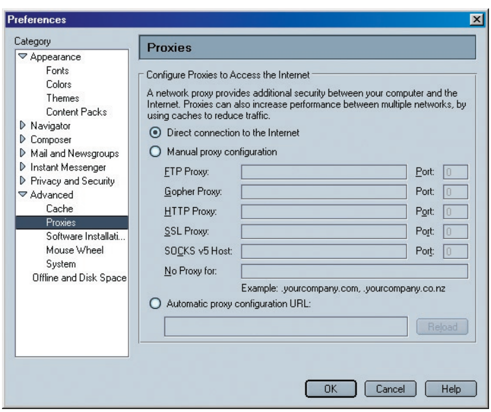
4. Accertarsi che non vi siano segni di spunta vicino a nessuna delle opzioni visualizzate: “Rileva automaticamente impostazioni” e “Utilizza un server proxy”. Fare clic su “OK”. Cliccare ancora su “OK” nella pagina delle “Opzioni Internet”.



Netscape Navigator versione 4.0 o successive

1. Avviare Netscape. Clic su “Modifica”, quindi su “Preferenze”.

2. Nella finestra delle preferenze, cliccare su “Avanzate”, quindi selezionare “Proxy”. Nella finestra “Proxy”, selezionare “Connessione diretta a Internet”.



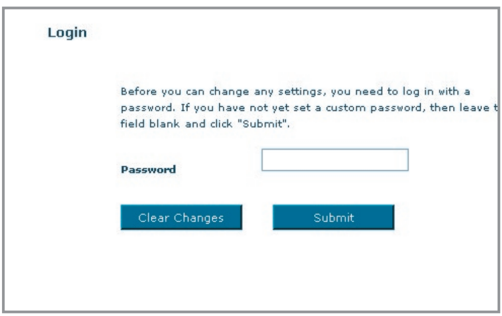
Esecuzione del programma di installazione guidata

1. Per accedere all'interfaccia utente di gestione del router basata sul web, utilizzare il browser web da un computer collegato al router. Nella barra di indirizzo del proprio browser, digitare “192.168.2.1” (non digitare niente del tipo “http://” o “www”) e premere il tasto “Enter” (Invio).



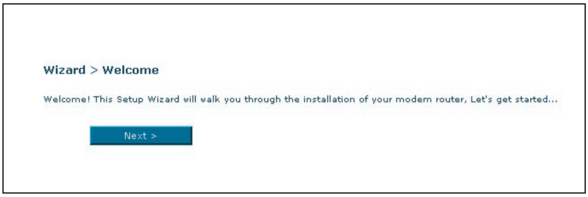
Nota bene: per la configurazione iniziale, si consiglia vivamente di utilizzare un computer fisicamente collegato al router tramite un cavo RJ45. Non è consigliabile utilizzare per la configurazione iniziale un computer collegato in modalità wireless.

2. Nel browser compare la seguente schermata che invita ad effettuare il login. Il router viene fornito senza alcuna password. Nella schermata di connessione, lasciare vuoto lo spazio per la password e fare clic su “Submit” (Inoltra) per connettersi.

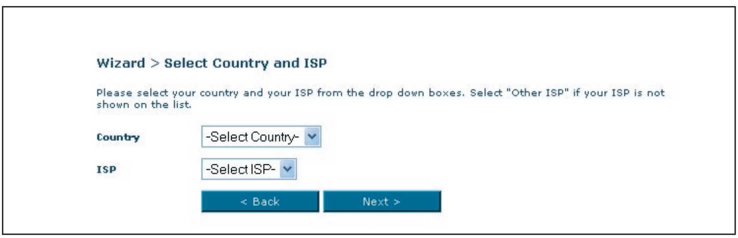


Nota bene:per maggiore sicurezza, si consiglia vivamente di cambiare la password. Per ulteriori informazioni su come cambiare la password e sulle altre opzioni di protezione, leggere la sezione intitolata “Configurazione manuale del router”.

3. La procedura di installazione guidata sarà avviata automaticamente per eseguire la configurazione rapida (consigliata). Fare clic su “Next” (Avanti) per continuare.



4. Il primo passaggio consiste nel selezionare il proprio Paese e ISP, quindi fare clic su “Next” (Avanti). Se il proprio Paese e/o ISP non fossero in elenco, selezionare “Other Country” (Altro Paese) oppure “Other ISP” (Altro ISP).



5 A questo punto digitare negli spazi vuoti il nome utente e la password forniti dal proprio provider Internet (ISP). Per eseguire la connessione, il nome utente e la password devono essere inseriti con esattezza. Il provider Internet confermerà il nome utente e la password.



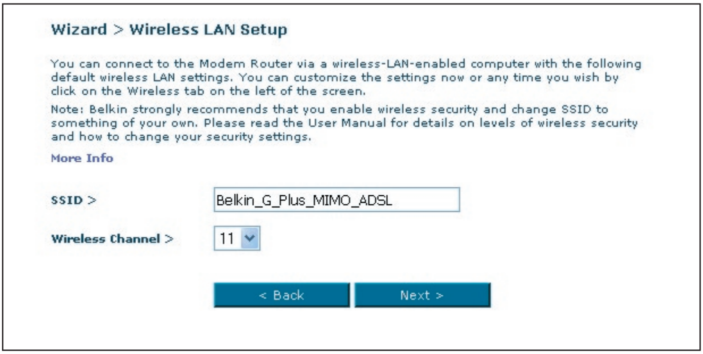
Nota bene: per istruzioni più dettagliate relative ad altri tipi di connessione, fare riferimento alla sezione intitolata “Configurazione manuale del router” di questo manuale.

6. Viene visualizzata la schermata di configurazione della rete LAN Wireless. Il collegamento con il router può essere eseguito tramite un computer con rete LAN wireless attivata con le seguenti impostazioni di rete LAN wireless predefinite:

SSID = Belkin G+ MIMO ADSL

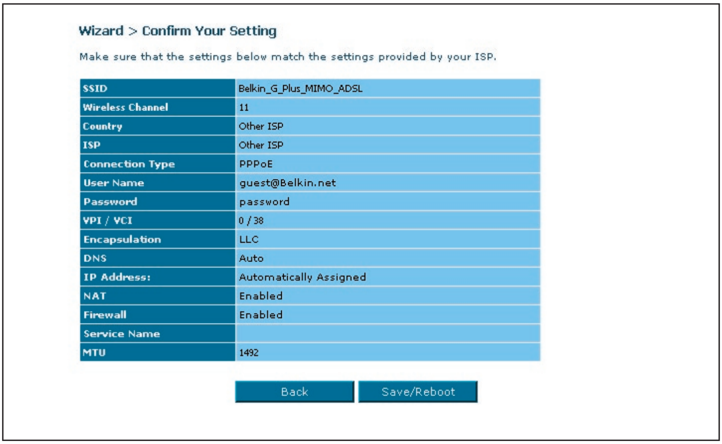
Canale Wireless = Auto

Protezione = disattivata



Nota bene: Belkin consiglia vivamente di attivare la protezione wireless WEP o WPA e cambiare a piacere l’SSID. Per ulteriori dettagli sui livelli di protezione wireless e su come modificare le impostazioni di sicurezza, vedere il Manuale Utente.

7. Controllare con attenzione le impostazioni riportate nella schermata successiva. Per modificare le impostazioni, fare clic su “Back” (Indietro) o fare clic su “Next” (Avanti) per confermarle.


Wizard > Confirm Your Setting

Make sure that the settings below match the settings provided by your ISP.

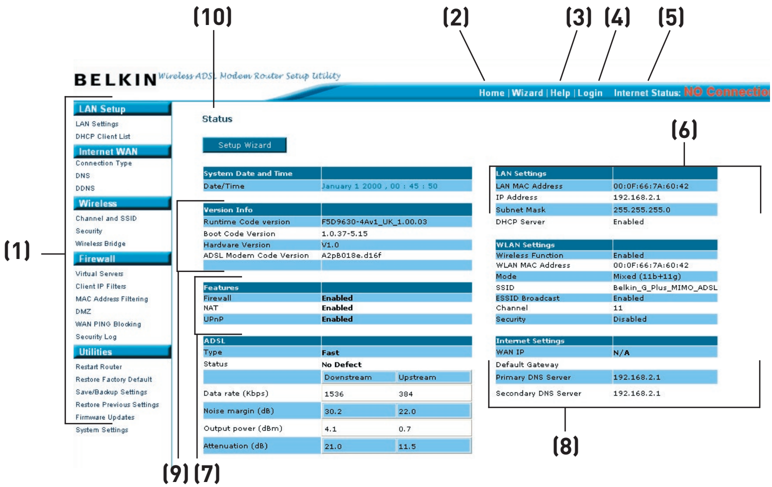
SSID	Belkin_G_Plus_MIMO_ADSL
Wireless Channel	11
Country	Other ISP
ISP	Other ISP
Connection Type	PPPoE
User Name	guest@Belkin.net
Password	password
VPI / VCI	0 / 38
Encapsulation	LLC
DNS	Auto
IP Address:	Automatically Assigned
NAT	Enabled
Firewall	Enabled
Service Name	
MTU	1492

Back | Save/Reboot

Nota bene: per modificare le proprie impostazioni, è possibile riavviare in qualsiasi momento l’impostazione guidata o utilizzare il menu di navigazione a sinistra.

Per una migliore comprensione dell'interfaccia utente avanzata basata sul web

Nella pagina principale viene riportata una breve sintesi dello stato e delle impostazioni del router. Da questa pagina è possibile accedere a tutte le pagine di impostazione avanzata.



1. Link di navigazione rapida

Facendo clic su questi link è possibile passare direttamente a qualsiasi altra pagina dell'interfaccia utente del router. I link sono suddivisi per categorie logiche e raggruppati per schede, in questo modo si facilita la ricerca di una particolare impostazione. Facendo clic sul titolo di ogni scheda appare una breve descrizione delle funzioni della scheda scelta.

2. Pulsante Home

Il pulsante "Home" è presente in ogni pagina dell'interfaccia utente. Premendo questo pulsante si ritorna alla pagina iniziale.

3. Pulsante Help

Il pulsante "Help" consente di accedere alle pagine guida del router. La guida è disponibile anche in molte pagine, è sufficiente fare clic su "more info" (maggiori informazioni) accanto ad alcune sezioni specifiche di ogni pagina.

4. Pulsante Login/Logout

Questo pulsante attiva e disattiva la connessione del router. Quando si è collegati al router, il pulsante riporta l'indicazione "Logout" (Disconnetti).

Collegandosi al router si viene condotti in una pagina di connessione a parte dove viene richiesta una password. Una volta collegati al router, è possibile modificare le impostazioni. Una volta terminate le modifiche, per scollegarsi dal router fare clic sul pulsante “Logout” (Disconnetti). Per maggiori informazioni sulla connessione al router, vi rimandiamo al capitolo “Connessione al router”.

5. **Indicatore di stato Internet**

   Questo indicatore è presente in tutte le pagine del router ed ha lo scopo di indicare lo stato del collegamento al router. Quando il messaggio “connection OK” (connessione ok) è VERDE, significa che il router è collegato ad Internet. Quando il router non è collegato ad Internet, appare il messaggio “no connection” (nessuna connessione) in ROSSO. L’indicatore viene aggiornato automaticamente modificando le impostazioni del router.

6. **Impostazioni LAN**

   Mostra le impostazioni della rete locale (Local Area Network - LAN) del router. Le impostazioni si possono modificare facendo clic sul collegamento di navigazione rapida LAN sulla sinistra della schermata.

7. **Funzioni**

   Visualizza lo stato delle caratteristiche UPnP, NAT e firewall del router. Per apportare delle modifiche, è sufficiente fare clic su uno qualsiasi dei link o sul link “Quick Navigation” (Navigazione rapida) nella parte sinistra dello schermo.

8. **Impostazioni Internet**

   Visualizza le impostazioni della sezione Internet/WAN del router che si collega a Internet. Per apportare eventuali modifiche, è sufficiente fare clic sul link di navigazione rapida “Internet/WAN” nella parte sinistra dello schermo.

9. **Informazioni sulla versione**

   Visualizza le informazioni relative alla versione del firmware, del bootcode, dell’hardware ed il numero di serie del router.

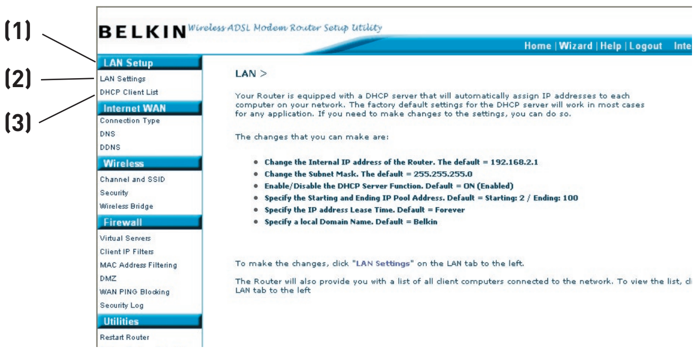
10. **Nome della pagina**

    Il nome che identifica la pagina in cui ci si trova. Questo manuale a volte farà riferimento alle pagine chiamandole per nome. Ad esempio, con “LAN > LAN Settings” (LAN > Impostazioni LAN) si intende la pagina “Impostazioni LAN”.

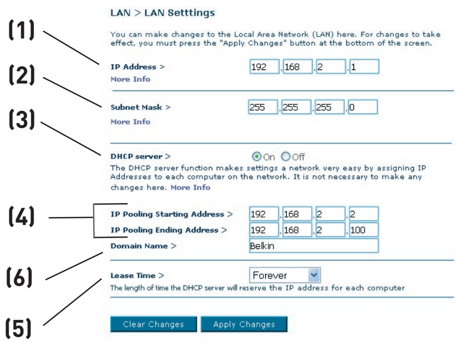
Modifica delle impostazioni LAN

Da qui possono essere visualizzate o modificate tutte le impostazioni di configurazione della LAN interna del router.

Facendo clic sul titolo della scheda LAN **(1)** si entra nella pagina di titolo della scheda LAN che contiene una rapida descrizione delle funzioni. Per visualizzare le impostazioni o modificare una qualsiasi delle impostazioni LAN, fare clic su “LAN Settings” **(2)** (Impostazioni LAN), o per visualizzare l’elenco dei computer collegati, fare clic su “DHCP client list” (Elenco client DHCP) **(3)**.



LAN Settings (Impostazioni LAN)



1. **Indirizzo IP**

   Per "Indirizzo IP" si intende l'indirizzo IP interno del router. L'indirizzo IP predefinito è "192.168.2.1". Per accedere all'interfaccia di configurazione, digitare l'indirizzo IP nell'apposita barra indirizzi del browser. Questo indirizzo, se necessario, può essere modificato. Per modificare l'indirizzo IP, digitare il nuovo indirizzo IP e fare clic su "Apply Changes" (Applica modifiche). L'indirizzo IP scelto dovrebbe essere un IP non instradabile. Esempi di indirizzi IP non instradabili sono:

   192.168.x.x (dove x indica qualsiasi cifra tra 0 e 255)

   10.x.x.x (dove x indica qualsiasi cifra tra 0 e 255)

2. **Maschera di sottorete**

   Non è necessario modificare la subnet mask, in quanto il router imposterà automaticamente la lunghezza in base al tipo di indirizzo IP.

3. **Server DHCP**

   La funzione server DHCP semplifica l'impostazione di una rete, in quanto gli indirizzi IP vengono assegnati automaticamente ad ogni computer nella rete. L'impostazione predefinita è "On" (Attiva). Il server DHCP può essere DISATTIVATO, se necessario, ma per farlo è necessario impostare manualmente un indirizzo IP statico per ogni computer in rete. Per disattivare il server DHCP, selezionare "Off" (disattivato) e fare clic su "Apply Changes" (Applica modifiche).

4. **Pool IP**

   Per "pool IP" si intende la gamma di indirizzi IP messa da parte per l'assegnazione dinamica dei computer alla rete. Il valore predefinito è 2–100

(99 computer). Per modificare questa cifra, digitare un nuovo indirizzo IP di inizio e fine e facendo clic su “Apply Changes” (Applica modifiche). Il server DHCP può assegnare automaticamente 100 indirizzi IP. Questo significa che non si può specificare un pool di indirizzi IP maggiore di 100 computer. Ad esempio, partendo da 50 significa che bisogna fermarsi a 150 o prima, in modo da non superare il limite dei 100 client. L’indirizzo IP di partenza deve essere un numero inferiore rispetto all’indirizzo IP finale.

5. **Lease Time**

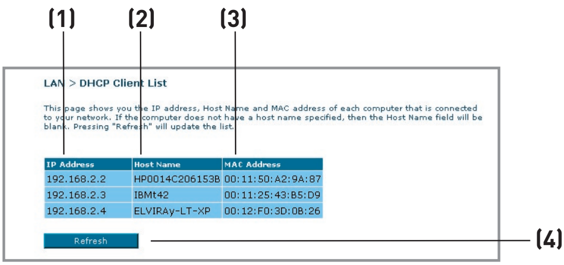
   Per “lease time” si intende la durata dell’intervallo durante il quale il server DHCP mantiene riservato l’indirizzo IP per ogni computer. È consigliabile lasciare questo intervallo impostato su “Forever” (Per sempre). L’impostazione predefinita “Forever” (Per sempre) sta ad indicare che ogni volta che ad un computer verrà assegnato un indirizzo IP dal server DHCP, l’indirizzo IP per quel particolare computer non cambierà più. Impostando intervalli minori, come un giorno o un’ora, una volta trascorso quello specifico intervallo gli indirizzi IP si libereranno. Questo significa anche che l’indirizzo IP di un particolare computer potrebbe cambiare nel corso del tempo. Eventuali altre opzioni avanzate del router, tra cui DMZ o filtri IP client, dipendono dall’indirizzo IP. Per questo motivo è bene che l’indirizzo IP non cambi.

6. **Local Domain Name**

   L’impostazione predefinita è “Belkin”. Per la propria rete è possibile impostare un dominio locale (nome della rete). Questa impostazione non deve essere necessariamente modificata a meno che non vi sia un’esigenza specifica per farlo. Alla rete può essere assegnato un nome qualsiasi, come ad esempio “MY NETWORK” (LA MIA RETE).

Elenco dei client DHCP

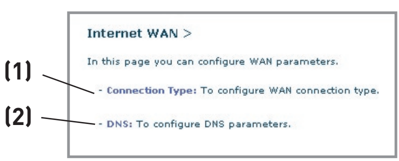
È possibile visualizzare un elenco dei computer (conosciuti come client) collegati alla rete. È possibile visualizzare l'indirizzo IP **(1)** del computer, il nome di host **(2)** (se al computer ne è stato assegnato uno), e l'indirizzo MAC **(3)** della scheda NIC (Network Interface Card). Premendo il pulsante "Refresh" (Ripristina) **(4),** l'elenco viene aggiornato. Nel caso fossero state fatte delle modifiche, l'elenco verrà aggiornato.



Internet WAN

Nella scheda "Internet/WAN" è possibile configurare il router per potersi collegare al proprio provider Internet (ISP). Il router è in grado di collegarsi praticamente a qualsiasi sistema di provider ADSL, a condizione che le impostazioni siano state configurate correttamente per il tipo di connessione al provider desiderato. Le impostazioni di connessione sono fornite dal provider stesso. Per configurare il router con le impostazioni indicate dal provider, fare clic su "Connection Type" (Tipo di connessione) **(1)** nel lato sinistro dello schermo. Selezionare il tipo di connessione utilizzato. Se il provider avesse fornito le impostazioni DNS, facendo clic su "DNS" **(2)** si possono inserire le informazioni relative all'indirizzo DNS per quei provider che richiedono alcune specifiche impostazioni.

Terminate queste impostazioni, l'indicatore "Internet Status" (Stato Internet), se il router è stato impostato correttamente, visualizzerà il messaggio "connection OK" (connessione OK).



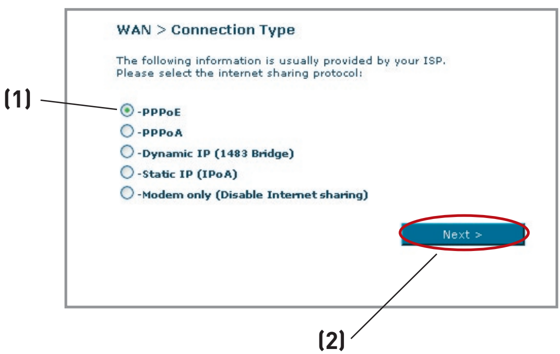
Tipo di connessione

Dalla pagina “Connection Type” (Tipo di connessione) è possibile scegliere tra cinque tipi di connessione sulla base delle istruzioni fornite dal proprio ISP:

- PPPoE
- PPPoA
- IP dinamico (con bridging 1483)
- IP statico (IPOA)
- Soltanto modem (disattivare la condivisione Internet)

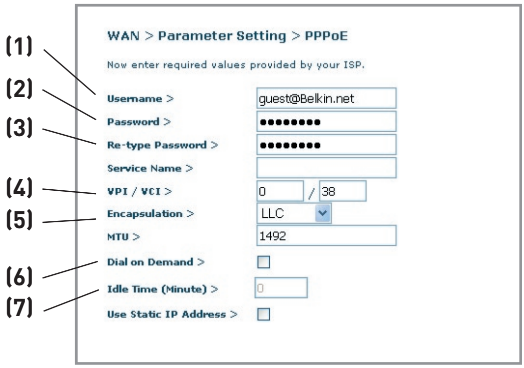
Nota bene: per conoscere alcuni dei parametri di impostazione Internet DSL comuni, vedere l’Appendice C di questo manuale. Nel dubbio, contattare il proprio ISP.

Selezionare il tipo di connessione utilizzata facendo clic sul pulsante di opzione**(1)** accanto al tipo di connessione e facendo quindi clic su “Next” (Avanti) **(2)**.



Configurazione del proprio tipo di connessione ISP su PPPoE o PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) rappresenta il metodo standard per collegare i dispositivi collegati in rete Per accedere alla rete del proprio ISP e collegarsi ad Internet questo tipo di connessione richiede un nome utente ed una password. Lo standard PPPoA (PPP over ATM) è simile allo standard PPPoE, ma è utilizzato principalmente nel Regno Unito. Selezionare PPPoE o PPPoA e fare clic su “Next” (Avanti). Quindi inserire le informazioni fornite dal proprio ISP e fare clic su “Apply Changes” (Applica modifiche) per attivare le impostazioni.



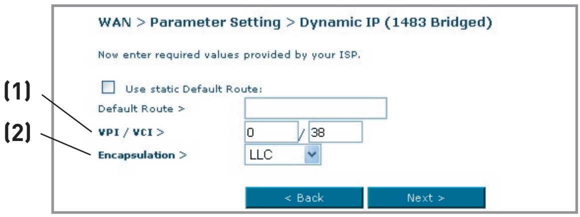
1. **User Name -** digitare il nome utente. (forniti dal proprio ISP).
2. **Password -** Digitare la password. (forniti dal proprio ISP).
3. **Retype Password (Ridigita password) -** Confermare la password (fornita dal proprio ISP).
4. **VPI/VCI -** Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI) (forniti dal proprio ISP).
5. **Encapsulation (Incapsulamento) -** Scegliere il tipo di incapsulamento (fornito dal proprio ISP) per specificare come gestire i protocolli multipli sul livello di trasporto ATM.

   VC-MUX: Lo standard PPPoA Virtual Circuit Multiplexer (incapsulamento nullo) consente di avere un solo protocollo in funzione per ciascun circuito virtuale con un numero inferiore di overhead.

   LLC: Lo standard PPPoA Logical Link Control consente a diversi protocolli multipli di funzionare su un unico circuito virtuale (maggior numero di overhead).
6. **Dial on Demand (Composizione a richiesta) -** Selezionando l’opzione “Dial on Demand” il router si collegherà automaticamente ad Internet ogni volta che un utente aprirà un browser web
7. **Idle Time (Minutes) (Intervallo di inattività - Minuti) -** Indicare il tempo di inattività massimo per la connessione a Internet. Superato questo intervallo, la connessione verrà interrotta.

Configurazione del tipo di connessione su IP dinamico (con bridging 1483)

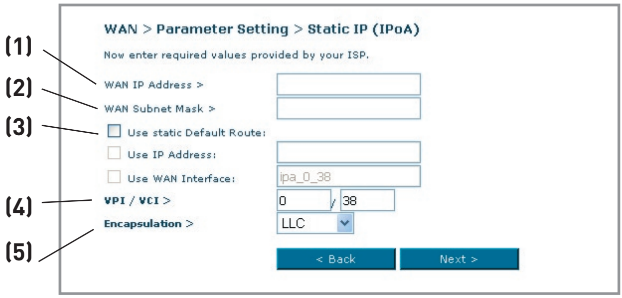
Questo metodo di connessione consente di creare un ponte di collegamento tra la propria rete e quella dell'ISP. Il router riceve l'indirizzo IP automaticamente dal server DHCP dell'ISP.



1. **VPI/VCI -** Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). Questi parametri di identificazione vengono assegnati dall'ISP.
2. **Encapsulation (Incapsulamento)** Selezionare i parametri LLC o VC MUX utilizzati dall'ISP.

Impostazione del proprio tipo di connessione ISP sull'IP statico (IPoA)

Questo tipo di connessione viene anche chiamato "Classical IP over ATM" o "CLIP", ed è quello fornito dall'ISP come IP fisso del router da collegare ad Internet.

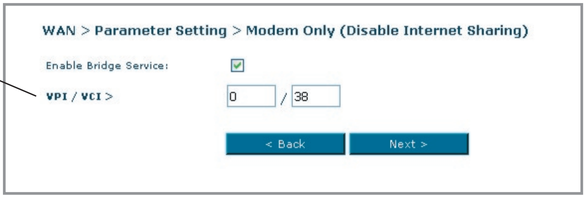


1. **WAN IP Address (Indirizzo IP WAN) –** Digitare un indirizzo IP assegnato dal proprio ISP per l'interfaccia WAN del router.
2. **WAN Subnet Mask -** Digitare una maschera di sottorete assegnata dal proprio ISP.
3. **Default Route (Percorso predefinito) -** Digitare un indirizzo IP gateway predefinito. Se il router non riesce a trovare l'indirizzo di destinazione entro la propria rete locale, trasmette i pacchetti al gateway predefinito assegnato dal proprio ISP.
4. **VPI/VCI -** Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). Questi parametri di identificazione vengono assegnati dall'ISP.
5. **Encapsulation (Incapsulamento)** Selezionare i parametri LLC o VC MUX utilizzati dall'ISP.

Impostare il tipo di connessione su Modem Only (Soltanto modem) disattivando la condivisione Internet

In questa modalità, il router agisce semplicemente come ponte per trasferire i pacchetti attraverso la porta DSL. Per accedere ad Internet è necessario disporre di altro software supplementare installato nei propri computer.

(1)

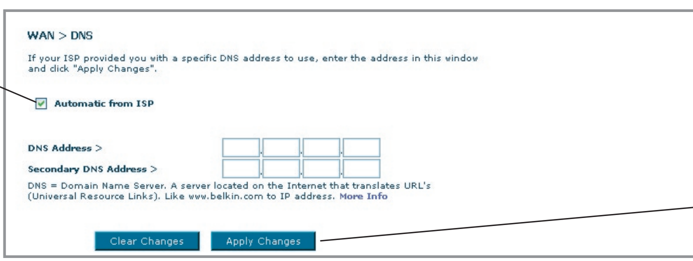


1. **VPI/VCI -** Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio ISP).

Impostazioni DNS (Domain Name Server)

Un “Domain Name Server” è un server presente in Internet che traduce gli Universal Resource Link (URL) come “www.belkin.com” in indirizzi IP. Molti ISP non richiedono l’immissione di questa informazione nel router. Se non è stato inserito alcun indirizzo DNS specifico, la casella “Automatic from ISP” **(1)** dovrebbe essere spuntata. Se si utilizza un tipo di connessione IP statica, perché la propria connessione funzioni correttamente, potrebbe essere necessario inserire uno specifico indirizzo DNS ed un indirizzo DNS secondario. Se il proprio tipo di connessione fosse di tipo dinamico o PPPoE, potrebbe non essere necessario inserire un indirizzo DNS. Lasciare la casella “Automatic from ISP” (Automatico da ISP) selezionata. Per digitare le impostazioni dell’indirizzo DNS, togliere il segno di spunta dalla casella “Automatic from ISP” (Automatico da ISP) e digitare i propri dati DNS negli spazi disponibili. Fare clic su “Apply Changes” (Applica modifiche) **(2)** per salvare le impostazioni.

(1)



(2)

Utilizzo del DNS dinamico

Il servizio Dynamic DNS (DNS dinamico) vi permette di trasformare un indirizzo IP dinamico in un nome host statico in uno qualsiasi dei domini offerti dalla DynDNS.org. Ciò permette di accedere ai computer di rete più facilmente da varie postazioni Internet. DynDNS.org offre questo servizio, per un massimo di 5 host name, gratuitamente alla comunità Internet.

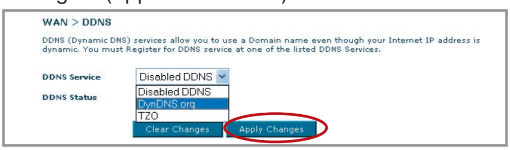
Il servizio “Dynamic DNSSM” è ideale per i siti web domestici, file server o per semplificare l’accesso ai file archiviati ed al PC in casa. Con questo servizio si può essere certi che il proprio nome host porti sempre al proprio indirizzo IP, anche se l’ISP lo cambia. Quando l’indirizzo IP cambia, rimanete localizzabili attraverso il sito dyndns.org.

Per registrarsi gratuitamente al servizio di nome host DNS dinamico, andare al link http://www.dyndns.org.

Impostazione dell’aggiornamento client del DNS dinamico del router

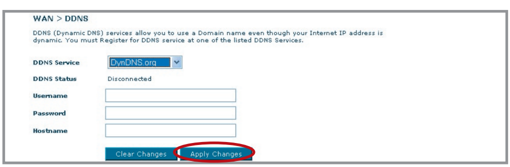
Prima di poter usufruire del servizio di aggiornamento gratuito, bisogna registrarsi con DynDNS.org. Una volta effettuata la registrazione, seguire le seguenti istruzioni:

1. Selezionare “DynDNS.org” dal menu a tendina. Fare clic su “Apply Changes” (Applica modifiche).



2. Inserire il proprio nome utente DynDNS.org nel campo “User Name” **(1)**.
3. Inserire la propria password DynDNS.org nel campo “Password / Key” **(2)**.
4. Nel campo “Domain Name”(Nome dominio) (3), digitare il nome del dominio DynDNS.org creato con DynDNS.org. **(3)**.
5. Fare clic su “Apply Changes” (Applica modifiche) per aggiornare l’indirizzo IP.

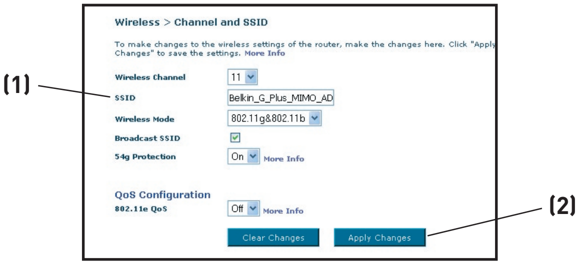
Ogni volta che l’indirizzo IP fornito dall’ISP cambia, il router aggiornerà automaticamente i server di DynDNS.org con il nuovo indirizzo IP. È possibile effettuare questa operazione anche manualmente, facendo clic sul pulsante “Apply Changes” (Applica modifiche) **(4)**.



Wireless

Nella scheda “Wireless” è possibile modificare le impostazioni di configurazione di rete. Da questa scheda è possibile modificare il nome della rete wireless (SSID), il canale operativo e le impostazioni di protezione crittografata.

Channel and SSID (Canale e SSID)



1. Modifica del canale wireless

Esistono numerosi canali operativi tra cui scegliere. Negli Stati Uniti i canali sono 11. Nel Regno Unito e in gran parte d’Europa i canali sono 13. In pochi altri paesi ancora i requisiti per i canali sono diversi. Il vostro router è stato configurato per funzionare sui canali adatti al paese in cui vivete. Il canale predefinito è 11. (Salvo che vi troviate in un paese che non consente l’impiego del canale 11). Questo canale, se necessario, può essere cambiato. In presenza di altre reti wireless nella stessa area, la rete dovrà essere impostata in modo da funzionare su un canale diverso dalle altre reti wireless. Per ottenere prestazioni migliori, utilizzare un canale che sia almeno a cinque canali di distanza dalle altre reti wireless. Ad esempio, in presenza di un’altra rete che funziona sul canale 11, impostare la propria rete sul canale 6 o su un canale minore. Per cambiare canale, selezionare il canale desiderato dal menu a tendina. Fare clic su “Apply Changes” (Applica modifiche). La modifica è immediata.

2. Modifica del nome della rete wireless (SSID)

Per identificare la propria rete wireless, si utilizza un nome chiamato SSID (Service Set Identifier). L’SSID predefinito del router è “belkin54g”. È possibile sostituire questo nome con un altro qualsiasi o lasciarlo invariato. In presenza di altre reti wireless nella stessa area, è consigliabile utilizzare un SSID unico (diverso da quello di un’eventuale altra rete wireless in zona). Per cambiare l’SSID, digitare nel campo SSID il nome desiderato **(1)** e fare clic su “Apply Changes” (Applica modifiche)**(2)**. La modifica è immediata. Nel caso il nome SSID venga modificato, è necessario riconfigurare anche i computer wireless per consentirne il collegamento al nuovo nome della rete. Per ulteriori indicazioni su come eseguire le modifiche necessarie, vedere la documentazione relativa alla scheda di rete wireless.

3. Utilizzo del servizio di trasmissione ESSID

Per questioni di sicurezza si può scegliere di non trasmettere la propria SSID di rete. In questo modo, il proprio nome di rete rimarrà nascosto a quei computer che eseguiranno un'analisi per rilevare la presenza di eventuali reti wireless. Per disattivare il servizio di trasmissione SSID, togliere il segno di spunta dalla casella accanto all'opzione Broadcast SSID. La modifica è immediata. A questo punto, tutti i computer devono essere impostati in modo da potersi collegare al proprio SSID specifico; un SSID "QUALSIASI" non sarà più accettato. Per ulteriori indicazioni su come eseguire le modifiche necessarie, vedere la documentazione relativa alla scheda di rete wireless.

Nota bene: questa funzione avanzata dovrebbe essere scelta soltanto dagli utenti esperti.

4. Utilizzo dello switch di modalità wireless

Il router può funzionare in due diverse modalità wireless:

- **802.11b & 802.11g-** Scegliere questa opzione se si pensa di connettere alla propria rete dei client wireless 802.11b e 802.11g
- **802.11g -** Usare questa modalità se non vi sono clienti 802.11b all'interno della rete. Questa opzione offre le migliori prestazioni, tuttavia non permette il collegamento ai clienti 802.11b.

5. Commutazione in modalità protetta

Una parte della specifica 802.11g prevede che la modalità protetta garantisca il corretto funzionamento dei client e punti di accesso 802.11g in presenza di un pesante traffico 802.11b nell'ambiente operativo. Quando la modalità protetta è ATTIVA, il dispositivo 802.11 verifica la presenza di altro traffico di rete prima di provvedere alla trasmissione dei dati. Pertanto, utilizzata negli ambienti con un PESANTE traffico 802.11b o in presenza di interferenze, questa modalità garantisce prestazioni migliori. In un ambiente dove il traffico di rete wireless è molto ridotto o assente, le prestazioni migliori si ottengono con la modalità protetta DISATTIVATA.

Crittografia/Sicurezza

Protezione della rete Wi-Fi

Di seguito sono descritte alcune soluzioni per rendere più efficiente la rete wireless e per proteggere i propri dati da intrusioni indesiderate. Questo capitolo è dedicato agli utenti che usano la rete da casa, dall'ufficio in casa e da piccoli uffici. Al momento della stampa di questo manuale, i tipi di crittografia disponibili sono tre.

Nome	64 bit Wired Equivalent Privacy	128 bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronimo	64-bit WEP	128-bit WEP	WPA-TKIP/AES (oppure soltanto WPA)	WPA2-AES (oppure soltanto WPA2)
Protezione	Buona	Migliore	Ottima	Ottima
Caratteristiche	Chiavi statiche	Chiavi statiche	Crittografia a chiavi dinamiche e autenticazione reciproca	Crittografia a chiavi dinamiche e autenticazione reciproca
	Chiavi di crittografia basate sull'algoritmo RC4 (generalmente chiavi a 40 bit)	Più sicura rispetto alla protezione WEP a 64 bit con una chiave lunga 104 bit, più 24 bit aggiuntivi dei dati generati dal sistema	Protocollo TKIP (temporal key integrity protocol) aggiunto per permettere la rotazione delle chiavi e il potenziamento della crittografia	La crittografia AES (Advanced Encryption Standard) non provoca alcuna perdita di trasferimento dati

WEP (Wired Equivalent Privacy)

Il protocollo WEP (Wired Equivalent Privacy) potenzia la protezione di tutti i prodotti wireless conformi allo standard Wi-Fi. Questo protocollo comune offre alle reti wireless lo stesso livello di protezione della privacy di una rete cablata simile.

WEP a 64 bit

La protezione 64-bit WEP fu introdotta per la prima volta con la crittografia da 64 bit, che prevedeva una lunghezza di chiave di 40 bit più altri 24 bit supplementari di dati generati dal sistema (per un totale di 64 bit). Alcuni produttori di hardware chiamarono la protezione a 64 bit crittografia a 40 bit. Poco tempo dopo l'introduzione della tecnologia, i ricercatori scoprirono che la crittografia a 64 bit poteva essere decodificata molto facilmente.

WEP a 128 bit

Per riparare alle potenziali debolezze della crittografia WEP a 64 bit, fu quindi progettato un metodo più sicuro a 128 bit. La crittografia a 128 bit comprende una chiave da 104 bit più 24 bit aggiuntivi di dati generati dal sistema (128 bit in totale). Alcuni produttori di hardware chiamarono la protezione a 128 bit crittografia a 104 bit.

La maggior parte delle apparecchiature wireless attualmente in commercio supporta entrambi i tipi di crittografia, a 64 e 128 bit, tuttavia alcune apparecchiature più vecchie supportano solo la WEP a 64 bit. Tutti i prodotti wireless Belkin supportano entrambi i tipi di crittografia, a 64 e 128 bit.

Chiavi di crittografia

Dopo aver scelto tra la modalità di crittografia “64-bit” oppure “128-bit WEP” è fondamentale generare una chiave di crittografia. La chiave di crittografia dovrà essere sempre la stessa per tutta la rete wireless, altrimenti i dispositivi di rete wireless non saranno in grado di comunicare tra loro e l’utente non sarà in grado di comunicare all’interno della rete.

La chiave di crittografia può essere inserita manualmente in modalità esadecimale, oppure inserendo una frase di accesso nel campo “Passphrase” (frase di accesso) e cliccando quindi sulla richiesta di generare la chiave. Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 64 bit è necessario inserire una chiave composta da 10 caratteri esadecimali. Per la protezione WEP a 128 bit, vanno inseriti 26 caratteri esadecimali.

La frase di accesso WEP NON è la stessa cosa della chiave WEP. La scheda wireless fornita utilizza la frase di accesso per generare le chiavi WEP, ma i metodi per generare le chiavi potrebbero cambiare a seconda del produttore. Se nella rete sono presenti dispositivi di varie marche, la cosa più semplice da fare è usare la chiave WEP esadecimale del router o dell’access point wireless ed inserirlo manualmente nella tabella dei codici esadecimali WEP nella schermata di configurazione della scheda.

Utilizzo di una chiave esadecimale

Una chiave esadecimale è composta da numeri e lettere che vanno dalla A alla F e dallo 0 al 9. Le chiavi a 64 bit sono composte da cinque numeri a due cifre. Le chiavi a 128 bit sono composte da 13 numeri a due cifre.

Ad esempio:

AF 0F 4B C3 D4 = chiave a 64-bit

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = chiave a 128 bit

Nelle caselle riportate di seguito va creata la propria chiave, inserendo in ogni casella due caratteri compresi tra A-F e 0–9. Questa chiave sarà utilizzata per programmare le impostazioni di crittografia del router e dei propri computer wireless.

Nota per gli utenti Mac: i prodotti originali Apple AirPort supportano soltanto la crittografia a 64 bit. I prodotti Apple Airport 2 supportano sia la modalità di crittografia a 64 che a 128 bit. Verificare quale sia la versione utilizzata. Non potendo configurare la rete con una crittografia a 128 bit, provare una crittografia a 64 bit.

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) è un nuovo standard Wi-Fi che offre maggiore sicurezza rispetto alle caratteristiche di crittografia WEP. Per poter utilizzare la protezione WPA, i driver ed il software dell'apparecchiatura wireless devono essere aggiornati in maniera adatta a supportarla. Tali aggiornamenti sono disponibili nel sito web del rivenditore dei dispositivi wireless. Esistono due tipi di protezione WPA: WPA-Personal (PSK) e WPA-Enterprise (RADIUS).

WPA-Personal (PSK)

Questo metodo si avvale di una chiave pre-condivisa come chiave di rete. Una chiave di rete pre-condivisa è una password la cui lunghezza varia da 8 a 63 caratteri, tra lettere, numeri ed altri caratteri. Ogni client usa la stessa chiave di rete per accedere alla rete. Generalmente, questa è la modalità utilizzata in un ambiente domestico.

WPA-Enterprise (RADIUS)

Questo sistema consente ad un radius server di distribuire automaticamente la chiave di rete ai client. Generalmente, questa modalità viene utilizzata in un ambiente di lavoro. Un elenco dei prodotti wireless Belkin che supportano la protezione WPA è riportato al sito web **www.belkin.com/networking**.

WPA2 (WiFi Protected Access)

WPA2 è la seconda generazione dello standard 802.11i basato su WPA. Offre un maggiore livello di protezione combinando un'autenticazione di rete avanzata ed un metodo di crittografia AES rafforzato. Come per la protezione WPA, la protezione WPA2 è disponibile sia nella modalità Personal (PSK) sia nella modalità Enterprise (RADIUS). Solitamente, la modalità WPA2-Personal è quella più diffuso nelle reti domestiche, mentre la modalità WPA-Enterprise viene utilizzata più spesso in aziende dove un server radius distribuisce automaticamente la chiave di rete ai client.

Condivisione dei codici di rete

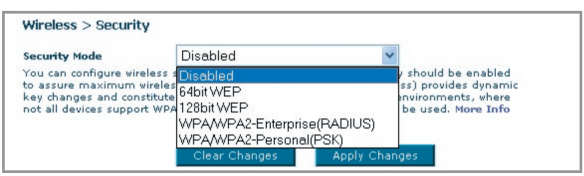
Nella maggior parte dei prodotti Wi-Fi la sicurezza è disattivata. Una volta messa in funzione la rete, sarà necessario attivare la protezione WEP o WPA2 ed assicurarsi che tutti i dispositivi wireless usino la stessa
chiave di rete.

La scheda di rete wireless G+ MIMO per desktop non può accedere alla rete perché usa una chiave di rete diversa da quella configurata nel router G+ MIMO wireless.



Modifica delle impostazioni di protezione della rete wireless

Il vostro router è protetto da crittografia WPA/WPA2 (Wi-fi Protected Access), il più recente standard di protezione wireless Esso supporta anche lo standard di protezione legacy WEP (Wired Equivalent Privacy). L'impostazione predefinita prevede che la protezione wireless sia disattivata. Per abilitare la protezione, è necessario stabilire prima lo standard che si desidera utilizzare. Per accedere alle impostazioni di protezione, **fare clic su "Security" (Protezione) nella scheda Wireless.**



Configurazione WEP

Crittografia WEP a 64 bit

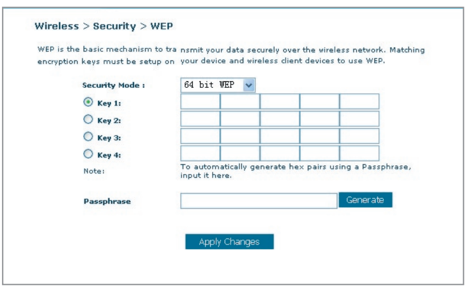
1. Selezionare “64-bit WEP” dal menu a tendina.

2. Una volta selezionata la modalità di crittografia WEP, sarà possibile inserire la propria chiave esadecimale digitandola manualmente.

Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 64 bit è necessario inserire una chiave composta da 10 caratteri esadecimali.

Ad esempio:

AF 0F 4B C3 D4 = chiave WEP a 64 bit



3. Fare clic su “Apply Changes” (Applica modifiche) per terminare. La crittografia del router è impostata. Ogni computer presente nella rete wireless deve essere configurato con le medesime impostazioni di protezione..

AVVERTENZA: se si stesse eseguendo la configurazione del router o dell’access point wireless da un computer con un client wireless, si perderà il collegamento fino a quando la protezione del client wireless non sarà stata attivata. Accertarsi di annotare la propria chiave prima di eseguire le modifiche

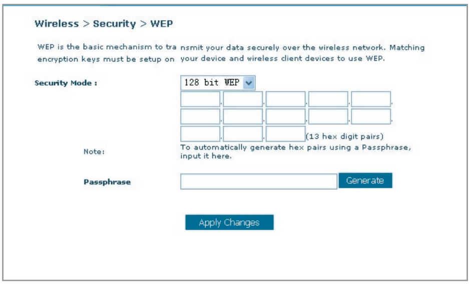
Crittografia WEP a 128 bit

1. Selezionare “128-bit WEP” dal menu a tendina.
2. Una volta selezionata la modalità di crittografia WEP, sarà possibile inserire la propria chiave esadecimale digitandola manualmente.

   Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit è necessario inserire una chiave composta da 26 caratteri esadecimali.

   Ad esempio:

   C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = chiave WEP a 128 bit



3. Fare clic su “Apply Changes” (Applica modifiche) per terminare. La crittografia del router è impostata. Ogni computer presente nella rete wireless deve essere configurato con le medesime impostazioni di protezione..

AVVERTENZA: se si stesse eseguendo la configurazione del router o dell’access point wireless da un computer con un client wireless, si perderà il collegamento fino a quando la protezione del client wireless non sarà stata attivata. Accertarsi di annotare la propria chiave prima di eseguire le modifiche.

Configurazione WPA

Nota bene: per utilizzare la protezione WPA, tutti i client devono disporre dei driver e del software in grado di supportarla. Al momento della pubblicazione di questo manuale, un security patch di Microsoft è disponibile gratuitamente, adatto soltanto al sistema operativo Windows XP. È necessario inoltre scaricare dal sito di supporto Belkin il driver più recente per la propria scheda di rete wireless G per computer desktop o

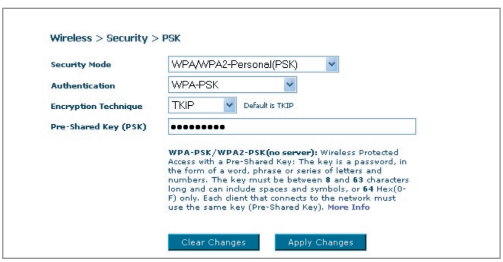
notebook Belkin. Attualmente gli altri sistemi operativi non sono supportati. Il patch Microsoft supporta esclusivamente i dispositivi che prevedono driver con la funzione WPA abilitata, tra cui i prodotti 802.11g Belkin.

Esistono due tipi di protezione WPA: WPA-Personal (PSK) e WPA-Enterprise (RADIUS). La protezione WPA-Personal (PSK) sfrutta la cosiddetta chiave precondivisa come codice di protezione. Una chiave pre-condivisa è una password la cui lunghezza varia da 8 a 63 caratteri, tra lettere, numeri ed altri caratteri. Ogni client usa lo stesso codice per accedere alla rete. Generalmente, questa modalità viene utilizzata in un ambiente domestico.

La protezione WPA-Enterprise (RADIUS) è una configurazione nell'ambito della quale un radius server distribuisce automaticamente le chiavi ai client. Questa soluzione viene generalmente utilizzata nell'ambiente lavorativo.

Impostazione della protezione WPA-Personal (PSK)

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA/WPA2-PSK.
2. Selezionare "WPA-PSK" per l'autenticazione.
3. Come "Encryption Technique" (tecnica di crittografia), scegliere "TKIP". Questa impostazione dovrà essere identica per tutti i client configurati.
4. Inserire la propria chiave precondivisa Questo codice può essere composto da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati. Ad esempio, la propria PSK potrebbe essere qualcosa del tipo: "Codice rete famiglia Rossi".



5. Fare clic su "Apply Changes" (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Impostazione WPA-Enterprise (RADIUS)

Se la vostra rete utilizza un radius server per distribuire le chiavi ai client, utilizzare questa impostazione.

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA/WPA2-Enterprise (RADIUS).

2. Selezionare “WPA-RADIUS” per l’autenticazione

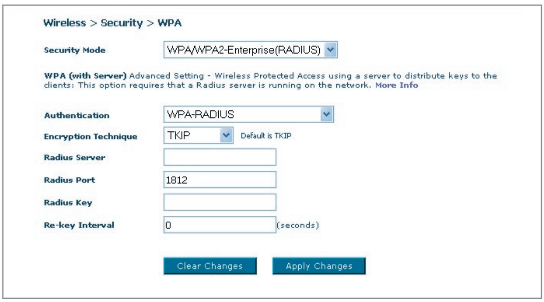
3. Come “Encryption Technique” (tecnica di crittografia), scegliere “TKIP”. Questa impostazione dovrà essere identica sui client configurati

4. Digitare l’indirizzo IP del radius server nei campi “Radius Server”.

5. Digitare la chiave radio nel campo “Radius Key”.

6. Digitare l’intervallo chiave. L’intervallo chiave indica la frequenza di distribuzione delle chiavi (in pacchetti).

7. Fare clic su “Apply Changes” (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.



Requisiti WPA2

IMPORTANTE: Per utilizzare la protezione WPA2, tutti i computer e gli adattatori di rete devono essere aggiornati con patch, driver e programmi di utilità che supportano la WPA2. Al momento della pubblicazione di questo manuale, è possibile scaricare gratuitamente un paio di security patch da Microsoft Questi patch sono adatti soltanto al sistema operativo Windows XP. Attualmente gli altri sistemi operativi non sono supportati.

Per i computer con Windows XP che non hanno Service Pack 2 (SP2), è possibile scaricare gratuitamente un file da Microsoft chiamato “Windows XP Support Patch for Wireless Protected Access (KB 826942)”.

Per Windows XP con Service Pack 2, Microsoft mette a disposizione un download gratuito per aggiornare i componenti del client wireless in modo da poter supportare la protezione WPA2 (KB893357). L’aggiornamento può essere scaricato dal sito: http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

IMPORTANTE: È necessario accertarsi inoltre che il produttore della scheda/ adattatori wireless supporti la protezione WAP2 e di aver scaricato e installato il driver più recente. Per la maggior parte delle schede wireless Belkin è possibile scaricare un driver di aggiornamento dal sito Belkin: www.belkin.com/networking

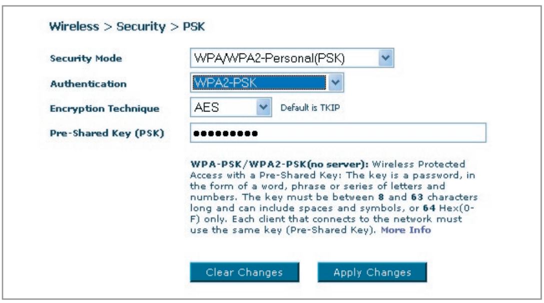
Impostazione della protezione WPA2-Personal (PSK)

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA/WPA2-PSK (PSK)".

2. Selezionare "WPA2-Personal (PSK)" per l'autenticazione.

3. Come "Encryption Technique" (tecnica di crittografia), scegliere "AES". Questa impostazione dovrà essere identica per tutti i client configurati.

4. Digitare la propria chiave precondivisa, Questo codice può essere composto da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati. Ad esempio, la propria PSK potrebbe essere qualcosa del tipo: "Codice rete famiglia Rossi".



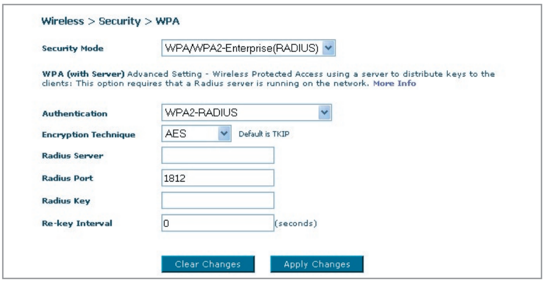
5. Fare clic su "Apply Changes" (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Impostazione WPA2-Enterprise (RADIUS)

Se la vostra rete utilizza un radius server per distribuire le chiavi ai client, utilizzare questa impostazione.

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA/WPA2-Enterprise (RADIUS)".
2. Selezionare "WPA2-RADIUS" per l'autenticazione
3. Come "Encryption Technique" (tecnica di crittografia), scegliere "AES". Questa impostazione dovrà essere identica sui client configurati

4. Digitare l'indirizzo IP del radius server nei campi "Radius Server".
5. Digitare la chiave radio nel campo "Radius Key".
6. Digitare l'intervallo chiave. L'intervallo chiave indica la frequenza di distribuzione delle chiavi (in pacchetti).
7. Fare clic su "Apply Changes" (Applica modifiche) per terminare. Ora devono essere configurati tutti i client in modo da essere adattati a queste impostazioni.



IMPORTANTE: Accertarsi che i computer wireless siano stati aggiornati in modo tale da poter funzionare con la protezione WPA2 e che le impostazioni siano corrette per poter effettuare la connessione con il router.

Configurazione dell'adattatore di rete per l'utilizzo della protezione

Nota bene: questa sezione contiene le informazioni su come configurare un adattatore di rete per utilizzare la protezione. A questo punto il router e l'access point wireless dovrebbero essere stati già configurati per l'utilizzo della crittografia WPA2, WPA o WEP. Per ottenere una connessione wireless, bisognerà configurare le schede di rete wireless notebook e desktop con le medesime impostazioni di protezione.

Le schede di rete wireless G+ MIMO Belkin dispongono di un programma di utilità di rete wireless. Cliccare sul nome della rete wireless (SSID) dall'elenco delle reti disponibili e digitare la chiave pre-condivisa (PSK). Per maggiori informazioni, vi preghiamo di consultare il manuale d'uso della scheda di rete Belkin.

Sulla maggior parte dei computer è possibile configurare il router dalla finestra "Proprietà di rete wireless" presente nel sistema operativo di Windows. Qui di seguito mostriamo due esempi:

Collegamento del computer a una rete wireless che richiede una chiave WEP a 64 o 128 bit

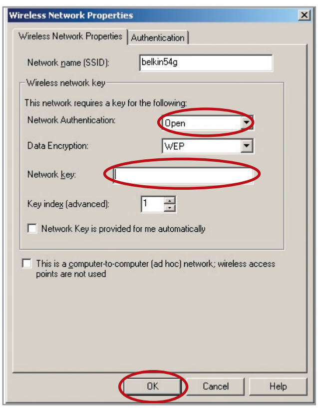
1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda wireless.

2. Nella scheda "Wireless Network Properties" , selezionare un nome dall'elenco "Available networks" (Reti disponibili) e fare clic su "Configure" (configura).

3. In "Data Encryption" (Crittografia dati), selezionare "WEP".

4. Disattivare la casella in basso "Network key is provided for me automatically" (Fornisci automaticamente la chiave di rete). Se si usa il computer per collegarsi ad una rete aziendale, chiedere al proprio amministratore di rete se la casella deve essere attivata.

5. Digitare la chiave WEP nella casella "Network key" (Chiave di rete).



Importante: una chiave WEP è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit, bisogna inserire 26 caratteri. Per la protezione WEP a 64 bit, bisogna inserire 10 caratteri. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

6. Fare clic su "OK" per salvare le impostazioni.

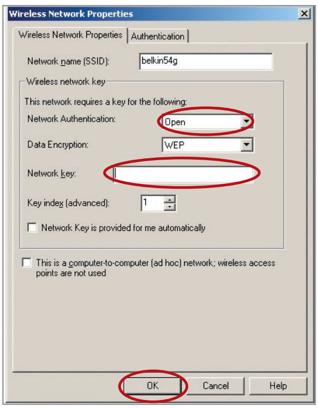
Collegamento del computer ad una rete wireless che usa la protezione WPA-PSK (senza server)

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda wireless.

2. Nella scheda "Wireless Network", selezionare un nome dall'elenco "Available networks" (Reti disponibili) e fare clic su "Configure" (configura).

3. In "Network Authentication" (Autenticazione di rete) selezionare "WPA-PSK (No Server)".

4. Digitare la chiave WPA nella casella "Network key" (Chiave di rete).



Importante: una chiave WPA-PSK è composta da numeri e lettere, da 0 a 9 e dalla A alla Z. Per la protezione WPA-PSK, si possono inserire da 8 a 63 chiavi. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

5. Fare clic su "OK" per salvare le impostazioni.

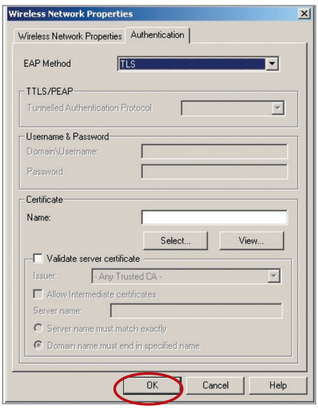
Collegamento del computer ad una rete wireless che usa la protezione WPA (con radius server)

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda wireless.

2. Nella scheda "Wireless Network", selezionare un nome dall'elenco "Available networks" (Reti disponibili) e fare clic su "Configure" (configura).

3. In "Network Authentication" (Autenticazione di rete) selezionare "WPA".

4. Nella scheda "Authentication" (Autenticazione), selezionare le impostazioni indicate dall'amministratore di rete.



5. Fare clic su "OK" per salvare le impostazioni.

Impostazione della protezione WPA/WPA2 per schede wireless di altre marche

Per le schede di rete wireless WPA desktop e notebook di altre marche sprovviste del software WPA/WPA2, è possibile scaricare gratuitamente un file da Microsoft chiamato "Windows XP Support Patch for Wireless Protected Access".

Nota: il file messo a disposizione da Microsoft funziona soltanto con Windows XP. Attualmente gli altri sistemi operativi non sono supportati.

Importante: È necessario accertarsi inoltre che il produttore della scheda wireless supporti la protezione WPA/WPA2 e di aver scaricato e installato il driver più recente dal suo sito.

Sistemi operativi supportati: • Windows XP Professional
• Windows XP Home Edition

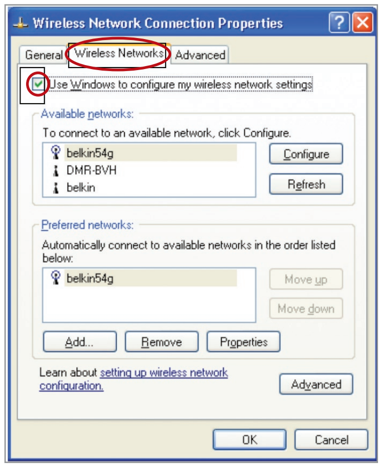
Impostazione della utility wireless Windows XP per utilizzare la protezione WPA/WPA2-PSK

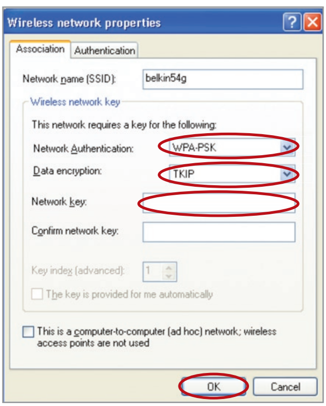
Per utilizzare la protezione WPA-PSK, accertarsi di utilizzare la utility di rete wireless Windows nel seguente modo:

1. In Windows XP, fare clic su “Start > Pannello di controllo > Connessioni di rete.

2. Con il tasto destro del mouse, fare clic sull’opzione “Connessione rete wireless”, e selezionare “Proprietà”.

3. Cliccando sulla scheda “Reti wireless” si aprirà la seguente schermata. Accertarsi che l’opzione “Utilizza Windows per configurare le impostazioni di rete wireless” sia selezionata.





4. Nella scheda “Reti wireless”, cliccare il pulsante “Configura” e si visualizzerà la seguente schermata.

5. Nel caso di una rete domestica o simile, selezionare “WPA-PSK” o WPA-PSK da “Autenticazione rete”.

Nota bene: selezionare “WPA” se si sta utilizzando il computer per collegarsi ad una rete aziendale che supporta un server di autenticazione come può essere un radius server. Per ulteriori informazioni, rivolgersi all’amministratore di rete.

6. Selezionare "TKIP" o "AES" da "Crittografia dati". Questa impostazione dovrà essere identica a quella del router configurato.

7. Digitare la propria chiave di crittografia nella casella "Chiave di rete".

Importante: inserire la propria chiave precondivisa Questo codice può essere composto da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati.

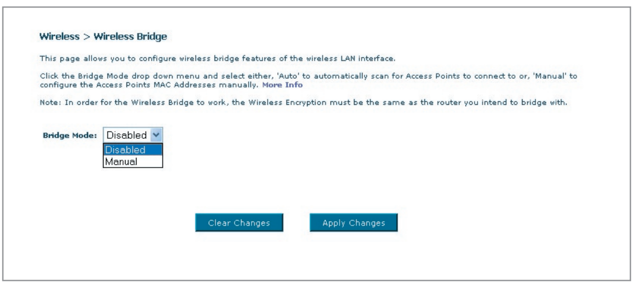
8. Fare clic su "OK" per confermare le impostazioni.

Bridge wireless

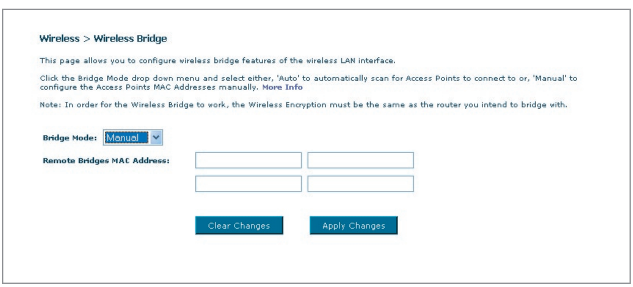
Le soluzioni Wireless Bridging o Wireless Distribution System (WDS) servono a collegare i router e gli access point wireless tra loro per ampliare una rete.

Fare clic sul menu a tendina accanto alla didascalia 'Bridge Mode' per scegliere tra:

Disabled (Disattivato): per disattivare la modalità Wireless Bridging (predefinita)



Manuale: per inserire manualmente l'indirizzo(i) MAC wireless degli access point ai quali collegarsi.



1 I canali wireless del router devono corrispondere a quelli dell'AP.

2 Le impostazioni di protezione (WEP) del router devono corrispondere a quelle dell'AP.

3 Se la filtrazione MAC è attiva, è necessario accertarsi di aggiungere l' indirizzo/i WLAN MAC del router/AP per consentire la comunicazione tra i due.

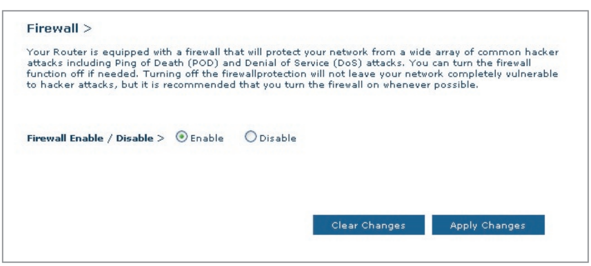
4 Se si utilizza una rete con protezione WPA, entrambi gli access point devono avere lo stesso SSID.

Firewall

Il router è dotato di una protezione firewall che salvaguarda la rete da una vasta gamma di comuni attacchi degli hacker, tra cui:

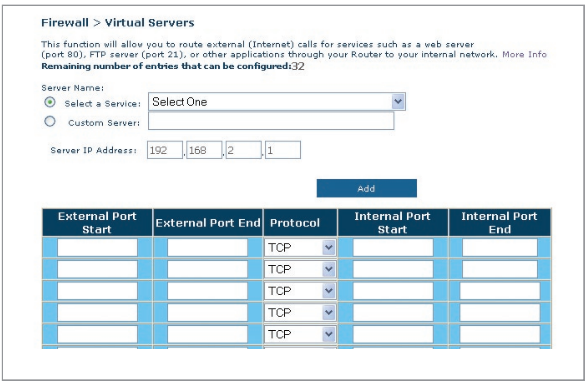
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

La protezione firewall inoltre maschera le porte comuni generalmente utilizzate per attaccare le reti. Queste porte appaiono "nascoste", il che significa che un potenziale hacker non le rileva. Se necessario, la funzione di protezione firewall può essere disattivata, ma è consigliabile lasciarla attiva. Disattivando la protezione firewall, la rete non rimarrà completamente vulnerabile agli attacchi degli hacker, ma è comunque indicato lasciare la protezione firewall attiva.



Server virtuali

I server virtuali consentono di instradare eventuali richieste di servizio esterne (di Internet), tra cui le richieste di vari servizi come quello di un server web (porta 80), server FTP (porta 21) o altre applicazioni attraverso il proprio router nella rete interna. Poiché i computer interni sono protetti da una protezione firewall, i computer di Internet non possono accedervi perché non li "vedono". Se fosse necessario configurare una funzione di server virtuale per una specifica applicazione, si dovrà contattare il fornitore dell'applicazione per conoscere le impostazioni delle porte necessarie. Le informazioni relative a queste porte si possono inserire nel router manualmente.



Scelta di un'applicazione

Sono previste diverse applicazioni comuni tra cui scegliere. Fare clic su "Select a Service" (Seleziona un servizio) e scegliere l'applicazione desiderata dall'elenco a tendina. Le impostazioni saranno trasferite alla riga specificata. Fare clic su "Add" (Aggiungi) per salvare le impostazioni per quella specifica applicazione.

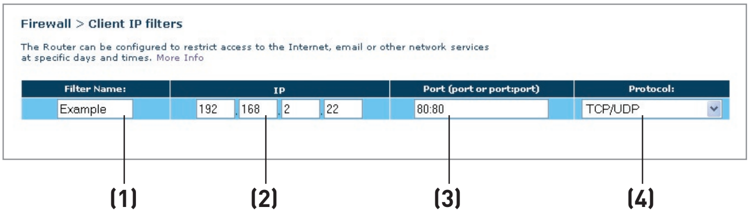
Immissione manuale delle impostazioni nel server virtuale

Per inserire manualmente le impostazioni, fare clic su "Custom Server" (Server personalizzato) ed inserire il nome per il server. Digitare l'indirizzo IP del server nello spazio previsto per la macchina interna e la(e) porta(e) da superare. Quindi selezionare il tipo di protocollo (TCP o UDP), quindi fare clic su "Add" (Aggiungi).

L'apertura delle porte nella protezione firewall può comportare un rischio per la sicurezza. Le impostazioni possono essere attivate e disattivate molto rapidamente. È consigliabile disattivare le impostazioni quando non si utilizza un'applicazione specifica.

Filtri IP Client

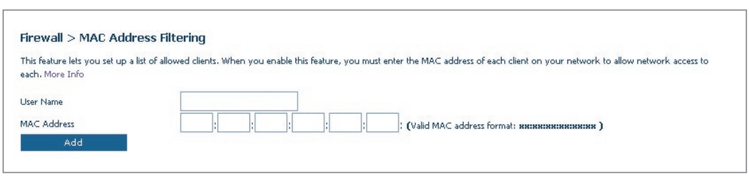
Il router può essere configurato in modo da limitare l'accesso ad Internet, alla posta elettronica o ad altri servizi di rete in particolari giorni o momenti.



Per limitare l'accesso ad Internet ad un solo computer ad esempio, inserire un nome del filtro nella casella "Filter Name" (Nome filtro) **(1)** e l'indirizzo IP del computer per il quale si desidera limitare l'accesso nel campo IP **(2)**. Quindi, digitare "80:80" nel campo Port (Porta) **(3)**. Selezionare il protocollo dalla casella a tendina "Protocol"
(4). Fare clic su "Apply Changes" (Applica modifiche). Al computer corrispondente all'indirizzo IP specificato sarà ora impedito l'accesso ad Internet.

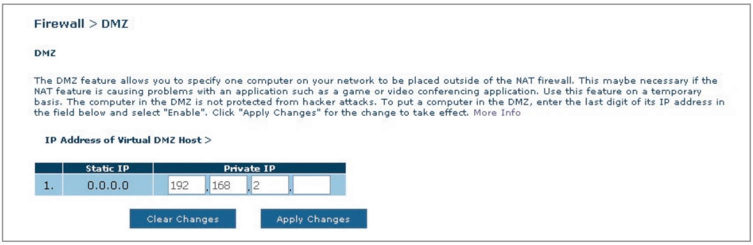
Il filtro indirizzi MAC

Il filtro indirizzi MAC è un potente mezzo per specificare quali sono i computer che possono accedere alla rete. Sarà negato l'accesso a qualsiasi computer che dovesse tentare di accedere alla rete e che non fosse specificato nell'elenco dei filtri. Quando questa opzione viene attivata, per consentire l'accesso alla rete ad ogni client, è necessario digitare un nome per l'utente e l'indirizzo MAC. Fare clic su "Add" (Aggiungi) per salvare le impostazioni.



DMZ (Demilitarized Zone)

Se si ha un PC client che non è in grado di gestire adeguatamente un'applicazione Internet da dietro una protezione firewall, per il client è possibile aprire un accesso a Internet illimitato a due vie. Questa operazione potrebbe essere necessaria qualora la funzione NAT entrasse in conflitto con un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Utilizzare questa funzione solo provvisoriamente. **Il computer nella DMZ non è protetto dagli attacchi degli hacker.**

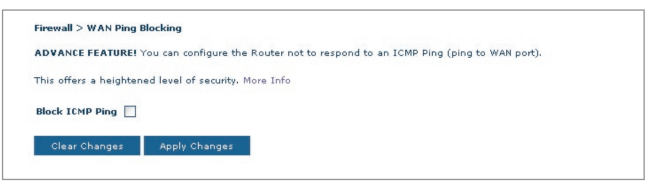


Per collocare il computer nella DMZ, digitare il rispettivo indirizzo IP LAN nel campo "Private IP" (IP Privato) e fare clic su "Apply Changes" (Applica modifiche) affinché la modifica venga attivata.

Blocco del ping ICMP

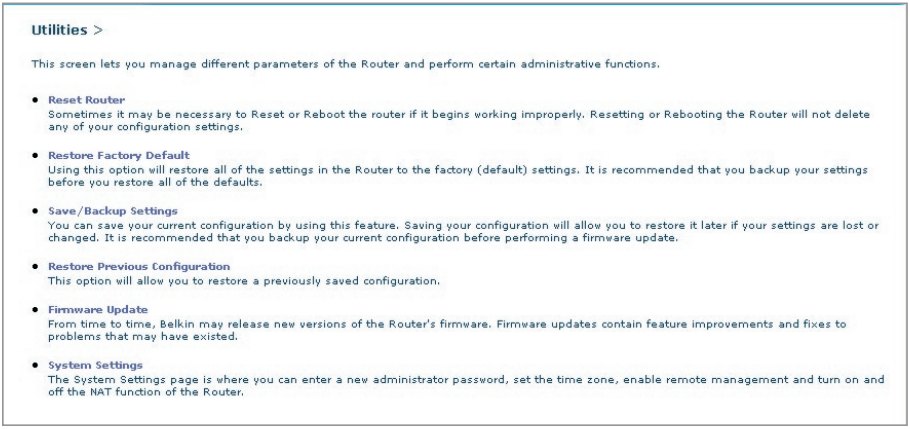
Gli hacker informatici utilizzano quello che è noto come "pinging" per scoprire le potenziali vittime in Internet. Colpendo uno specifico indirizzo IP e ricevendo una risposta da detto indirizzo IP, un hacker è in grado di stabilire se ci sia qualcosa di interessante o meno. Il router può essere impostato in modo da non rispondere ad un ping ICMP proveniente dall'esterno. In questo modo, il livello di protezione del proprio router aumenta.

Per disattivare la risposta al ping, selezionare "Block ICMP Ping" (Blocca ping ICMP) **(1)** e fare clic su "Apply Changes" (Applica modifiche). Il router in questo modo non reagirà se colpito da un ping ICMP.



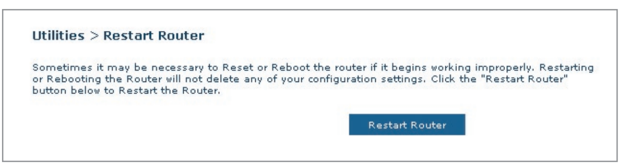
Utility

La schermata “Utility” consente di gestire diversi parametri del router ed eseguire alcune specifiche funzioni amministrative.



Riavvio del router

A volte, se inizia a funzionare in modo scorretto, il router deve essere riavviato. Se il router dovesse essere riavviato, le impostazioni di configurazione NON saranno cancellate.



Riavvio del router per ripristinare il normale funzionamento

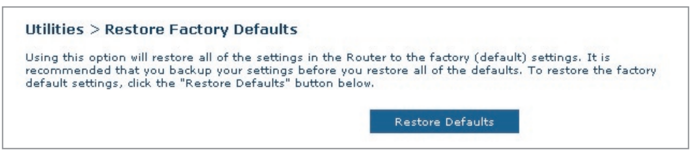
1. Fare clic sul pulsante “Restart Router” (Riavvia il router).

2. Compare il seguente messaggio. Fare clic su “OK” per riavviare il router.



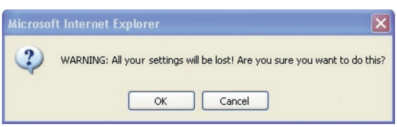
Ripristino delle impostazioni predefinite

Con questa opzione è possibile ripristinare tutte le impostazioni eseguite dal produttore del router. È consigliabile fare una copia di tutte le impostazioni prima di ripristinare quelle predefinite.



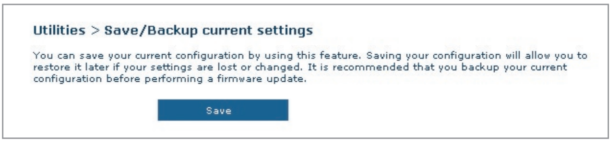
1. Fare clic sul pulsante “Restore Default” (Ripristina impostazioni predefinite).

2. Compare il seguente messaggio. Fare clic su “OK” per ripristinare le impostazioni predefinite.

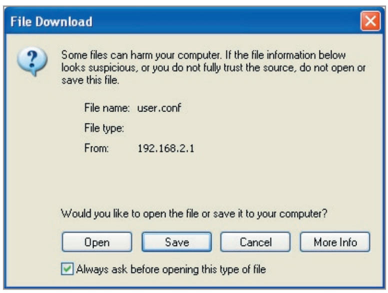


Salvataggio/Creazione di un copia di backup delle impostazioni correnti

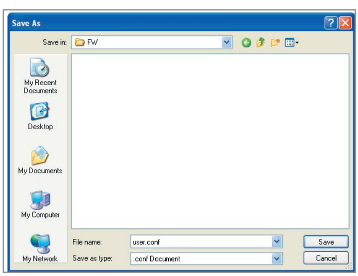
Questa opzione consente di salvare la configurazione attuale. Salvando la configurazione corrente è possibile ripristinarla in un momento successivo nel caso le impostazioni andassero perdute o venissero modificate. È consigliabile fare una copia della configurazione corrente prima di eseguire un aggiornamento del firmware.



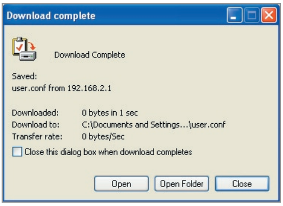
1. Fare clic su “Save” (Salva). Compare una finestra chiamata “File Download”. Fare clic su “Save” (Salva).



2. Si apre una finestra che consente di selezionare la posizione in cui salvare il file di configurazione. Selezionare una posizione. Non ci sono limiti rispetto al nome del file, tuttavia è necessario assegnare un nome che si è certi di ricordare anche in un momento successivo. Una volta selezionata la posizione ed il nome del file, fare clic su “Save” (Salva).



3. A salvataggio terminato, compare la finestra illustrata di seguito. Fare clic su “Close” (Chiudi).

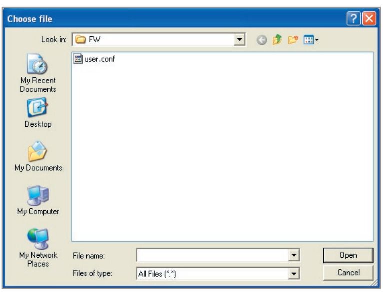


La configurazione è stata salvata.

Ripristino delle impostazioni precedenti

Questa opzione consente di ripristinare qualsiasi configurazione salvata in precedenza.

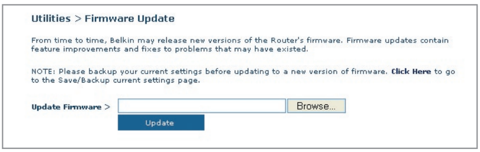
1. Fare clic su “Browse” (Sfoglia). Si apre una finestra che consente di selezionare la posizione del file di configurazione. Tutti i file di configurazione terminano con “.conf”. Trovare il file di configurazione che si desidera ripristinare e fare doppio clic su di esso.



2. Quindi, fare clic su “Open” (Apri).

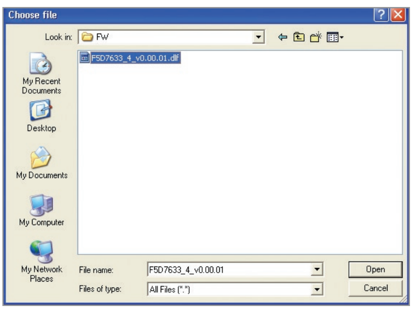
Aggiornamenti del firmware

Di tanto in tanto, Belkin potrebbe pubblicare nuove versioni del firmware del router. Gli aggiornamenti del firmware contengono alcuni miglioramenti e consentono di risolvere possibili problemi esistenti nelle versioni precedenti. I nuovi firmware pubblicati da Belkin si possono scaricare dal sito Belkin, aggiornando in questo modo il firmware del router alla versione più recente.



Aggiornamento del firmware del router

1. Dalla pagina “Firmware Update” (Aggiornamento firmware), fare clic su “Browse” (Sfoglia). Si apre una finestra che consente di selezionare la posizione del file di aggiornamento firmware.



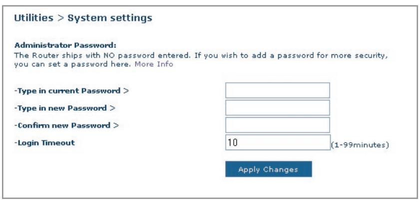
2. Andare al file di firmware scaricato. Selezionarlo facendo doppio clic sul nome del file.
3. Fare clic su “Update” (Aggiorna) per ottenere la più recente versione del firmware.

Impostazioni del sistema

Nella pagina “System Settings” è possibile inserire una nuova password per l’amministratore, impostare il fuso orario, attivare la gestione a distanza ed attivare e disattivare la funzione UPnP del router.

Impostazione o modifica della password amministratore

Il router viene fornito SENZA password. Se si desidera impostare una password per avere una maggiore protezione, lo si può fare da qui. La password deve essere annotata e custodita in un posto sicuro, in quanto sarà necessaria per connettersi al router in futuro. È anche consigliabile inserire una password nel caso si intenda utilizzare l’opzione di gestione a distanza del router.



Modifica della durata di connessione

L’opzione di durata connessione consente di impostare un intervallo di tempo di connessione all’interfaccia avanzata di impostazione del router. Il timer parte dal momento in cui non si rileva alcuna attività. Ad esempio, se fosse stata apportata qualche modifica all’interfaccia di impostazione avanzata, il computer si gestirà da solo senza dover fare clic su “Logout”. Supponendo che la durata di connessione sia stata impostata su 10 minuti, dopo 10 minuti di mancato utilizzo del computer, la sessione di connessione verrà interrotta. Per apportare ulteriori modifiche sarà quindi necessario connettersi di nuovo al router. L’opzione di durata della connessione è prevista a scopo cautelativo ed è preimpostata su 10 minuti.

Nota bene: è possibile connettere all’interfaccia avanzata di impostazione del router soltanto un computer alla volta.

Impostazione dell'ora e del fuso orario

Il router aggiorna l'orario collegandosi ad un server SNTP (Simple Network Time Protocol). In questo modo il router è in grado di sincronizzare l'orologio del sistema con la rete Internet mondiale. L'orologio sincronizzato presente nel router viene utilizzato per registrare l'elenco di protezione e controllare il filtro client.

Selezionare i server di orario NTP desiderati ed il proprio fuso orario, quindi fare clic su " Apply Changes" (Applica modifiche). L'orologio del sistema potrebbe non aggiornarsi immediatamente. Attendere almeno 15 minuti perché il router contatti i server dell'orario su Internet e riceva una risposta. L'utente non può impostare autonomamente l'orologio.



Attivazione della gestione a distanza

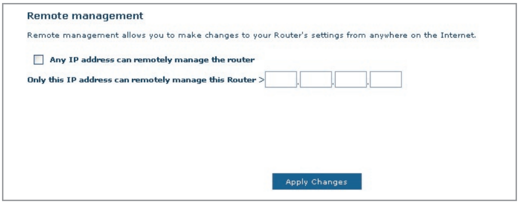
Prima di attivare questa funzione avanzata del router Belkin, **ACCERTARSI DI AVER IMPOSTATO LA PASSWORD AMMINISTRATORE.**. La gestione a distanza consente di modificare le impostazioni del router da qualsiasi punto di Internet.

Fare clic sul pulsante "Change Settings" (Modifica impostazioni) per visualizzare la pagina "Remote Management" (Gestione a distanza).

Esistono due metodi per gestire a distanza il router. Il primo consente di accedere al router da qualsiasi punto di Internet selezionando "Any IP address can remotely manage the Router" (Qualsiasi indirizzo IP può gestire a distanza il router). Digitando il proprio indirizzo WAN IP da qualsiasi computer in Internet, compare una schermata di connessione nella quale è necessario digitare la password del proprio router.

Il secondo metodo consiste nel consentire soltanto ad uno specifico indirizzo IP di gestire a distanza il router. Questo metodo è più sicuro, ma meno comodo. Per utilizzare questo metodo, digitare l'indirizzo IP dal quale si sa di accedere al router nello spazio previsto e selezionare "Only this IP address can remotely manage the Router" (Soltanto questo indirizzo IP può gestire a distanza il router). Prima di attivare questa funzione è FORTEMENTE CONSIGLIATO aver impostato la propria password amministratore. Lasciando la password vuota, si apre potenzialmente il router ad eventuali intrusioni esterne.

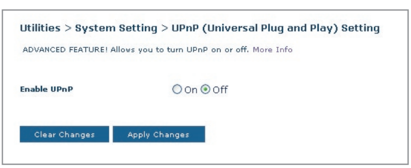
Fare clic su “Apply Changes” (Applica modifiche) per salvare le proprie impostazioni.



Abilitazione / disabilitazione del servizio UPnP

Il servizio UPnP (Universal Plug-and-Play) è un’altra opzione avanzata messa a disposizione dal router Belkin. Si tratta di una tecnologia in grado di offrire un funzionamento diretto delle opzioni di trasmissione di messaggi vocali, video, giochi ed altre applicazioni conformi agli standard UPnP. Per funzionare correttamente, alcune applicazioni richiedono che la protezione firewall del router sia configurata in maniera specifica. Per farlo è generalmente necessario aprire le porte TCP e UDP e, in alcuni casi, impostare le porte trigger. Un’applicazione conforme al servizio UPnP ha la capacità di comunicare con il router, fondamentalmente “dicendo” al router come configurare la protezione firewall. Il router viene fornito con l’opzione UPnP disabilitata. Se si sta utilizzando una qualsiasi applicazione conforme al servizio UPnP, e si desidera utilizzare le opzioni UPnP, queste si possono attivare.

Fare clic sul pulsante “Change Settings” (Modifica impostazioni) per visualizzare la pagina “UPnP Setting” (Impostazione UPnP). Quindi selezionare “On” per “Enable UPnP” (Abilita UPnP). Fare clic su “Apply Changes” (Applica modifiche) per salvare le proprie impostazioni.



Problema:

Il LED ADSL è spento.

Soluzione:

1. Controllare lo stato della connessione tra il router e la linea ADSL. Accertarsi che il cavo della linea ADSL sia collegato alla porta del router marcata "DSL Line".
2. Assicurarsi che il router sia alimentato. Il LED Power ⏻ (Alimentazione) sul pannello anteriore dovrebbe essere illuminato.

Problema:

Il LED Internet è spento.

Soluzione:

1. Accertarsi che il cavo della linea ADSL sia collegato alla porta del router marcata "DSL Line" e che il LED ADSL ☎ sia acceso.
2. Accertarsi di aver ricevuto i parametri VPI/VCI, nome utente e password corretti dal proprio ISP.

Problema:

Il mio tipo di connessione è "un indirizzo IP statico". Non riesco a collegarmi ad Internet.

Soluzione:

Se la vostra connessione prevede un indirizzo IP statico, il vostro ISP deve assegnarvi un indirizzo IP, una subnet mask e l'indirizzo gateway. Al posto di usare il programma di impostazione guidata, andare in "Connection Type" (Tipo di connessione) e selezionare il proprio tipo di connessione. Fare clic su "Next" (Avanti), selezionare "Static IP" (IP statico) e digitare il proprio indirizzo IP, la subnet mask e le informazioni relative al gateway predefinito.

Problema:

Ho dimenticato o smarrito la password.

Soluzione:

Premere per 10 secondi il pulsante "Reset" sul pannello posteriore per ripristinare le impostazioni predefinite.

Problema:

Il mio PC wireless non riesce a collegarsi al router.

Soluzione:

1. Accertarsi che le impostazioni SSID del PC wireless siano le stesse del router e che le impostazioni di sicurezza, come ad esempio la crittografia WPA o WEP, siano uguali per tutti i client.
2. Accertarsi che il router e il PC wireless non siano troppo distanti tra loro.

Problema:

La rete wireless si interrompe spesso.

Soluzione:

1. Avvicinare il PC wireless al router per ottenere un segnale migliore.
2. Ci potrebbero essere anche alcune interferenze, causate da un forno a microonde o dai telefoni cordless da 2,4 GHz. Spostare il router o utilizzare un canale wireless diverso.

Problema:

Non si riesce ad impostare un collegamento a Internet in modalità wireless.

Soluzione:

Nell'impossibilità di collegarsi ad Internet da un computer wireless, eseguire le seguenti verifiche:

1. Controllare lespie luminose sul router. Se si utilizza un router Belkin, le spie dovrebbero essere illuminate come segue:
   - La spia “Power” (Alimentazione) dovrebbe essere accesa.
   - Il LED “DSL” dovrebbe essere acceso, non lampeggiante.
   - Il LED “Internet LED” dovrebbe essere acceso o lampeggiante.
2. Aprire il software della utility wireless facendo clic sull'icona nel desktop di sistema nell'angolo in basso a destra dello schermo. Se si sta usando una scheda wireless Belkin, l'icona nel desktop del sistema dovrebbe apparire così  (l'icona può essere rossa o verde).
3. La finestra precisa che si apre varia in base al modello della scheda wireless in vostro possesso, tuttavia, qualsiasi utility dovrebbe prevedere un elenco delle reti disponibili (Available Networks), ovvero delle reti alle quali si può collegare .

Il nome della propria rete wireless appare nei risultati?

Sì, il nome della mia rete è in elenco passare alla soluzione per la risoluzione delle anomalie dal titolo “Non riesco a collegarmi ad Internet in modalità wireless, ma il nome della mia rete è in elenco”.

No, il nome della mia rete non è in elenco – passare alla soluzione dal titolo “Non riesco a collegarmi ad internet in modalità wireless e il nome della mia rete non è in elenco”.

Problema:

Non riesco a collegarmi ad internet in modalità wireless, ma il nome della mia rete è in elenco.

Soluzione:

Se il nome della rete appare nell’elenco “Available Networks”, seguire le seguenti indicazioni per collegarsi in modalità wireless:

1. Fare clic sul nome corretto della rete nell’elenco “Available Networks”.
2. Se la protezione (crittografia) della rete è stata attivata, bisognerà digitare la chiave di rete. Per ulteriori informazioni sulla protezione, vedere: “Modifica delle impostazioni di protezione della rete wireless”.
3. In pochi secondi, l’icona di sistema nell’angolo in basso a sinistra dello schermo dovrebbe diventare verde, indicando la corretta connessione alla rete.



Problema:

Non riesco a collegarmi ad internet in modalità wireless e il nome della mia rete non è in elenco

Soluzione

Se il nome corretto della rete non appare nell’elenco “Available Networks”, seguire le seguenti indicazioni per risolvere il problema:

1. Se possibile, spostare provvisoriamente il computer a 1,5/3 m dal router. Chiudere la utility Wireless ed aprirla di nuovo. Se il nome corretto della rete ora appare nell’elenco “Available Networks”, potrebbe trattarsi di un problema di copertura o di interferenza. Vedere i suggerimenti nell’allegato B intitolato “Considerazioni importanti per il posizionamento e la configurazione”.

2. Se si sta usando un computer collegato al router mediante un cavo di rete (anziché in modalità wireless), assicurarsi che la funzione “Broadcast SSID” (Trasmetti SSID) sia abilitata. Questa impostazione può essere trovata nella pagina di configurazione wireless “Channel and SSID” (Canale e SSID).

Se, dopo aver seguito queste istruzioni, non fosse ancora possibile accedere ad Internet, contattare l’Assistenza Tecnica Belkin.

Problema:

Il livello delle prestazioni della rete wireless non è buono

Il trasferimento dei dati a volte è lento.

Il segnale è debole.

Si incontrano difficoltà nell’impostare e/o mantenere una connessione con una rete VPN (Virtual Private Network)

Soluzione:

La tecnologia wireless è basata sulla tecnologia radio. Ciò significa che la connettività e le prestazioni di trasmissione tra i dispositivi diminuiscono all’aumentare della distanza. Altri fattori che possono causare un indebolimento del segnale (il metallo è generalmente l’indiziato numero uno) sono gli ostacoli quali muri e apparecchiature in metallo. Di conseguenza, la copertura tipica per i dispositivi wireless in un ambiente chiuso è compresa tra i 30 e i 60 metri. Inoltre, se ci si allontana ulteriormente dal router o dall’access point wireless, la velocità della connessione diminuisce.

Per determinare se i problemi wireless siano dovuti a fattori di copertura, provare a posizionare il computer a 1,5 metri e 3 metri di distanza dal router.

Cambiare il canale wireless - A seconda del traffico wireless locale e delle interferenze, cambiare il canale wireless della rete può migliorarne le prestazioni e l’affidabilità. Il canale predefinito del router è l’11, tuttavia, si possono scegliere altri canali, a seconda del paese nel quale ci si trova. Consultare il manuale a pagina 37 per le istruzioni su come scegliere altri canali wireless.

Limitazione della trasmissione dati wireless- Limitare la trasmissione dati può aiutare a migliorare la copertura wireless e la stabilità della connessione. La maggior parte delle schede di rete offre la possibilità di limitare la trasmissione dati. Per cambiare questa proprietà, andare sul pannello di controllo di Windows, aprire “Network Connections” (Connessioni di rete) e fare doppio clic sulla connessione della propria scheda wireless. Nella finestra di dialogo “Properties” (Proprietà), nella tabella “General” (Generale) selezionare il pulsante “Configure” (Configura) (gli utenti Windows 98 dovranno

selezionare la scheda wireless nell'elenco e quindi fare clic su "Properties" (Proprietà), quindi fare clic su la tabella "Advanced" (Avanzate) e selezionare le caratteristiche di trasmissione. Le velocità di trasmissione delle schede di rete dei client wireless sono generalmente preimpostate, tuttavia si possono verificare periodiche disconnessioni quando il segnale wireless è troppo basso. Generalmente, le velocità di trasmissione più lente sono le più stabili. Provare varie velocità fino a trovare la migliore per la propria rete; notare che tutte le trasmissioni di rete disponibili dovrebbero essere accettabili per la navigazione in Internet. Per maggiori dettagli consultare il manuale della scheda wireless.

Problema:

Si incontrano alcune difficoltà nell'impostare la protezione Wired Equivalent Privacy (WEP) in un router o access point Belkin

Soluzione

1. Collegarsi al router o all'access point.
2. Aprire il browser web e digitare l'indirizzo IP del router wireless o dell'access point. (Il router è preimpostato su 192.168.2.1, l'access point su 192.168.2.254). Collegarsi al router cliccando il pulsante "Login" nell'angolo in alto a destra dello schermo. Viene richiesto di inserire una password. Se non fosse mai stata impostata alcuna password, lasciare il campo password in bianco e cliccare "Submit" (Inoltra).
3. Fare clic su "Wireless" sul lato sinistro dello schermo. Selezionare la scheda "Encryption" (Crittografia) o "Security" (Protezione) per accedere alla pagina delle impostazioni di sicurezza.
4. Selezionare "128-bit WEP" dal menu a tendina.
5. Dopo aver selezionato la propria modalità di crittografia WEP, si può digitare a mano la propria chiave esadecimale WEP, oppure si può digitare una frase di accesso nel campo "Passphrase" (Frase di accesso) e fare clic su "Generate" per creare una chiave WEP dalla frase di accesso. Fare clic su Apply Changes (Applica modifiche) per terminare. Ora tutti i propri client vanno adattati a queste impostazioni. Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la sicurezza WEP a 128 bit, bisogna inserire una chiave di 26 caratteri esadecimali.

Ad esempio:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = chiave a 128 bit

6. Fare clic su "Apply Changes" (Applica modifiche) per terminare. La crittografia del router wireless è impostata. Ogni computer presente nella rete wireless deve essere configurato con le medesime impostazioni di protezione.

AVVERTENZA: se si stesse eseguendo la configurazione del router o dell'access point wireless da un computer con un client wireless, sarà necessario accertarsi che la protezione per questo client wireless sia attiva. In caso contrario si perderà la connessione wireless.

Nota per gli utenti Mac: i prodotti originali Apple AirPort ®supportano soltanto la crittografia a 64-bit. I prodotti Apple Airport 2 possono supportare la modalità di crittografia a 64 o 128 bit. Verificare quale sia la versione utilizzata nel proprio prodotto Apple AirPort. Non potendo configurare la rete con una crittografia a 128 bit, provare una crittografia a 64 bit.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wired Equivalent Privacy (WEP) in una scheda wireless Belkin.

Soluzione:

La scheda wireless deve utilizzare la stessa chiave del router wireless o dell'access point. FAd esempio, se il router wireless o l'access point utilizza la chiave 00112233445566778899AABBCC, la scheda wireless deve essere impostata esattamente con la stessa chiave.

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
2. Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
3. Dopo aver premuto il pulsante "Advanced", appare la Utility LAN Wireless Belkin. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda "Wireless Network Properties", selezionare un nome dall'elenco "Available networks" (Reti disponibili) e fare clic su "Properties" (Proprietà).
5. In "Data Encryption" (Crittografia dati), selezionare "WEP".

1 2 3 4 5 6 7 8 9 10 sezione

6. Disattivare la casella in basso “The key is provided for me automatically” (Fornisci automaticamente la chiave di rete). Se si usa il computer per collegarsi ad una rete aziendale, chiedere al proprio amministratore di rete se la casella deve essere attivata.
7. Digitare la chiave WEP nella casella “Network key” (Chiave di rete).

   Importante:una chiave WEP è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit, vanno inseriti 26 caratteri. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all’access point.

Ad esempio:
C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = chiave a 128 bit

8. Fare clic su “OK” e, quindi, su “Apply” (Applica) per salvare le impostazioni.

Se **NON** si utilizza una scheda wireless Belkin, richiedere al produttore il manuale d’uso per la scheda client wireless utilizzata.

Problema:

I prodotti Belkin supportano la modalità WPA?

Soluzione

Nota bene: per utilizzare la protezione WPA, tutti i client devono disporre dei driver e del software in grado di supportarla. Al momento della pubblicazione di questo elenco di domande e risposte, è possibile scaricare gratuitamente un security patch da Microsoft, adatto soltanto al sistema operativo Windows XP.

Il patch può essere scaricato al sito:

http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

Dal sito di assistenza Belkin è necessario anche scaricare il driver più recente per la propria scheda di rete wireless 802.11g desktop o notebook Belkin. Attualmente gli altri sistemi operativi non sono supportati. Il patch Microsoft supporta esclusivamente i dispositivi che prevedono driver con la funzione WPA abilitata, tra cui i prodotti 802.11g Belkin.

I driver più recenti si possono scaricare al sito: http://web.belkin.com/support/networkingsupport.asp.

Il supporto WPA sarà installato automaticamente nel caso si aggiornasse il proprio sistema alla versione Windows XP Service pack 2. Dettagli in merito sono riportati al sito http://support.microsoft.com

Problema:

Ho difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in un router o access point Belkin per una rete domestica.

Soluzione:

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA-PSK (no server)".
2. Come "Encryption Technique" (tecnica di crittografia), scegliere "TKIP" o "AES". Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare la propria chiave precondivisa, che può essere composta da una combinazione di lettere, numeri o caratteri o spazi, da un minimo di 8 a un massimo di 63. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati. Ad esempio, la propria PSK potrebbe essere qualcosa del tipo: "Chiave di rete famiglia Rossi".
4. Fare clic su "Apply Changes" (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in un router o access point Belkin per una rete aziendale.

Soluzione:

Se la vostra rete utilizza un radius server per distribuire le chiavi ai client, utilizzare questa impostazione. Questa soluzione viene generalmente utilizzata nell'ambiente lavorativo.

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA-PSK (with server)".
2. Come "Encryption Technique" (tecnica di crittografia), scegliere "TKIP" o "AES". Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare l'indirizzo IP del radius server nei campi "Radius Server".
4. Digitare la chiave radio nel campo "Radius Key".
5. Digitare l'intervallo chiave. L'intervallo chiave indica la frequenza di distribuzione delle chiavi (in pacchetti).
6. Fare clic su "Apply Changes" (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless Belkin per una rete domestica.

Soluzione:

I client devono utilizzare la stessa chiave del router wireless o dell'access point. Ad esempio, se la chiave è "Smith Family Network Key" nel router wireless router o nell'access point, anche i client devono utilizzare la stessa chiave.

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
2. Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
3. Una volta selezionato il pulsante "Advanced" (Opzioni avanzate), la utility wireless LAN Belkin appare automaticamente. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda "Wireless Network Properties", selezionare un nome dall'elenco "Available networks" (Reti disponibili) e fare clic su "Properties" (Proprietà).
5. In "Network Authentication" (Autenticazione di rete) selezionare "WPA-PSK (No Server)".
6. Digitare il codice WPA nella casella "Network key" (Codice rete).

Importante: una chiave WPA-PSK è composta da numeri e lettere, da 0 a 9 e dalla A alla Z. Per la protezione WPA-PSK, si possono inserire chiavi da 8 a 63 caratteri. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

7. Fare clic su "OK" e, quindi, su "Apply" (Applica) per salvare le impostazioni.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless Belkin per una rete aziendale.

Soluzione:

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
2. Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.

3. Una volta selezionato il pulsante “Advanced” (Opzioni avanzate), la utility wireless LAN Belkin appare automaticamente. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda “Wireless Network Properties”, selezionare un nome dall’elenco “Available networks” (Reti disponibili) e fare clic su “Properties” (Proprietà).
5. In “Network Authentication” (Autenticazione di rete), selezionare “WPA”.
6. Nella scheda “Authentication” (Autenticazione), selezionare le impostazioni indicate dall’amministratore di rete.
7. Fare clic su “OK” e, quindi, su “Apply” (Applica) per salvare le impostazioni.

Problema:

Si incontrano difficoltà nell’impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless**NON** Belkin per una rete domestica.

Soluzione:

Per le schede di rete wireless WPA desktop e notebook **NON** Belkin e sprovviste del software WPA, è possibile scaricare gratuitamente un file da Microsoft chiamato “Windows XP Support Patch for Wireless Protected Access”. Scaricare il patch da Microsoft ricercando nei dati base per Windows XP WPA.

Nota bene: il file messo a disposizione da Microsoft funziona soltanto con Windows XP. Attualmente gli altri sistemi operativi non sono supportati. È necessario accertarsi inoltre che il produttore della scheda wireless supporti la protezione WPA e di aver scaricato e installato il driver più recente dal suo sito.

Sistemi operativi supportati:

- Windows XP Professional
- Windows XP Home Edition

Attivazione dell’opzione WPA-PSK (senza server)

1. In Windows XP, fare clic su “Start > Pannello di controllo > Connessioni di rete”.
2. Cliccando con il tasto destro del mouse sulla scheda “Reti wireless si aprirà la seguente schermata. Accertarsi che l’opzione “Utilizza Windows per configurare le impostazioni di rete wireless” sia attivata.

3. Nella scheda “Reti wireless”, cliccare il pulsante “Configura” e si visualizzerà la seguente schermata.

4. Nel caso di una rete domestica o simile, selezionare “WPA-PSK” da “Amministrazione rete”.

Nota bene: selezionare “WPA (con radius server)” se si sta utilizzando il computer per collegarsi ad una rete aziendale che supporta un server di autenticazione come può essere un radius server. Per ulteriori informazioni, rivolgersi all’amministratore di rete.

5. Selezionare “TKIP” o “AES” da “Crittografia dati”. Questa impostazione deve essere identica a quella del router wireless o dell’access point configurato.

6. Digitare la propria chiave di crittografia nella casella “Chiave di rete”.

Importante: Inserire la propria chiave precondivisa Questo codice può essere composto da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati.

7. Fare clic su “OK” per confermare le impostazioni.

Qual è la differenza tra 802.11b, 802.11g, G+ MIMO e Pre-N?

Attualmente esistono quattro livelli di standard di rete wireless, che trasferiscono dati a velocità massime molto diverse tra loro. Ognuno di loro inizia per 802.11(x), nome dato loro dall’ IEEE, l’ente responsabile della certificazione degli standard di rete. Lo standard di rete wireless più comune, il 802.11b, trasferisce dati a 11 Mbps; l’802.11a e l’802.11g a 54 a 108 Mbps; G+ MIMO ha una velocità di 54 Mbps.

Tabella di confronto wireless

Tecnologia wireless	802.11b	G (802.11g)	G+ (802.11g con HSM)	G+ MIMO(802.11g con MIMO MRC)	Belkin Pre-N (802.11g con True MIMO)
Velocità*	11Mbps link rate / Baseline	5 volte più veloce dello standard 802.11b*	10 volte più veloce dello standard 802.11b*	10 volte più veloce dello standard 802.11b*	15 volte più veloce dello standard 802.11b*
Frequenza	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz
Compatibilità	Compatibile con 802.11g	Compatibile con: 802.11b/g	Compatibile con 802.11b/g	Compatibile con 802.11b/g	Compatibile con 802.11g o 802.11b
Copertura*	Normalmente 30 - 60m in ambienti chiusi	Fino a 120 metri*	Fino a 200 metri*	Fino a 300 metri*	Fino a 400 metri*
Vantaggi	Tecnologia legacy lungamente testata	Comune - ampio utilizzo della condivisione Internet	Velocità e copertura maggiori	Copertura maggiore e velocità costante	Leader nel settore - ottima copertura ed efficienza

*La distanza e le velocità di connessione variano in funzione dell'ambiente di rete.

Allegato A: Glossario

IP Address (Indirizzo IP)

Per “Indirizzo IP” si intende l’indirizzo IP interno del router. Per accedere all’interfaccia di impostazione avanzata, digitare l’indirizzo IP nell’apposita barra indirizzi del browser. Questo indirizzo, se necessario, può essere modificato. Per modificare l’indirizzo IP, digitare il nuovo indirizzo IP e fare clic su “Apply Changes” (Applica modifiche). L’indirizzo IP scelto dovrebbe essere un IP non instradabile. Esempi di indirizzi IP non instradabili sono:

192.168.x.x (dove x indica qualsiasi cifra tra 0 e 255)

10.x.x.x (dove x indica qualsiasi cifra tra 0 e 255)

Subnet Mask

Alcune reti sono troppo grandi per consentire che il traffico scorra in tutte le loro parti. Queste reti devono essere suddivise quindi in sezioni più piccole, meglio gestibili, dette sottoreti. La subnet mask (maschera di sottorete) è l’indirizzo accompagnato da altre informazioni necessarie ad identificare la “sottorete”.

DNS

DNS è l'acronimo di Domain Name Server. Un "Domain Name Server" è un server presente in Internet che traduce gli URL (Universal Resource Links) come "www.belkin.com" in indirizzi IP. Molti ISP non richiedono l'immissione di questa informazione nel router. Se si utilizza un tipo di connessione IP statica, perché la propria connessione funzioni correttamente, potrebbe essere necessario inserire uno specifico indirizzo DNS ed un indirizzo DNS secondario. Se il proprio tipo di connessione fosse dinamico o PPPoE, è probabile che non sia necessario inserire un indirizzo DNS.

PPPoE

La maggior parte dei provider ADSL utilizza un tipo di connessione PPPoE. Nel caso si utilizzasse un modem ADSL per collegarsi ad Internet, il proprio ISP potrebbe utilizzare il tipo di connessione PPPoE per collegarsi al servizio.

Il proprio tipo di connessione è PPPoE se:

1. Il proprio ISP ha fornito un nome utente ed una password per collegarsi alnternet.
2. Il proprio ISP ha fornito un software del tipo WinPOET o Enternet300 da utilizzare per collegarsi ad Internet
3. Per entrare in Internet, è necessario fare doppio clic su un'icona del desktop diversa da quella del proprio browser.

   Per impostare il router in modo da utilizzare il servizio PPPoE, digitare il proprio nome utente e la password negli appositi spazi. Dopo aver inserito i propri dati, fare clic su "Apply Changes" (Applica modifiche).

Una volta eseguite le modifiche, l'indicatore "Internet Status" (Stato Internet) visualizzerà il messaggio "Connection OK", se il router è stato impostato correttamente.

PPPoA

Digitare le informazioni PPPoA negli appositi spazi e fare clic su "Next" (Avanti). Fare clic su "Apply" (Applica) per attivare le impostazioni.

1. User name (Nome utente) - Digitare il nome utente. (forniti dal proprio ISP).
2. Password - Digitare la propria password (forniti dal proprio ISP).
3. Retype Password (Ridigita password) - Confermare la password. (fornita dal proprio ISP).
4. VPI/VCI - Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio ISP).

Disconnetti dopo X

Questa opzione viene utilizzata per disconnettere automaticamente il router dall'ISP quando non vi sono attività in corso per un intervallo di tempo specifico. Ad esempio, posizionando un segno di spunta accanto a questa opzione e digitando “5” nello spazio riservato ai minuti, si farà in modo che il router si disconnetta da Internet dopo cinque minuti di inattività di Internet. Questa opzione dovrebbe essere utilizzata nel caso il servizio di Internet venga pagato a minuti.

Channel and SSID (Canale e SSID)

Per cambiare canale, selezionare il canale di funzionamento del router dal menu a discesa e selezionare il proprio canale. Fare clic su “Apply Changes” (Applica modifiche) per salvare le impostazioni. È possibile modificare anche i parametri SSID. I parametri SSID sono l'equivalente del nome della rete wireless. I parametri SSID possono essere di qualsiasi tipo si desideri. In presenza di altre reti wireless nella propria area, assegnare alla propria rete wireless un nome univoco. Fare clic nella casella SSID e digitare un nuovo nome. Fare clic su “Apply Changes” (Applica modifiche) per salvare la modifica.

Trasmissione ESSID

Molte schede di rete wireless attualmente sul mercato prevedono una funzione detta “site survey”. Essa consente di esaminare attorno per rilevare qualsiasi rete disponibile e consentire al computer di selezionare la rete tramite la funzione di descrizione generale del sito. Questa condizione si verifica se l'SSID è impostato su “ANY” (QUALSIASI). Il router Belkin può bloccare questa ricerca casuale di una rete. Disattivando la funzione di trasmissione “ESSID Broadcast”, l'unico modo in cui un computer è in grado di entrare nella rete è tramite la propria SSDI impostata con il nome specifico della rete (WLAN ad esempio). Accertarsi di conoscere i propri parametri SSID (nome della rete) prima di attivare questa opzione. È possibile rendere la propria rete wireless quasi invisibile. Disattivando la trasmissione SSID, la rete non sarà rilevata. Naturalmente, disattivando la trasmissione SSID, la protezione aumenta.

Crittografia

Utilizzando la funzione di crittografia, la rete viene resa più sicura. Per proteggere i vostri dati, il router sfrutta la crittografia Wired Equivalent Privacy (WEP) e WIFI protested Access (WPA) e prevede due gradi di protezione: a 64 bit e a 128 bit. La crittografia si basa su un sistema di chiavi. La chiave inserita nel computer deve corrispondere alla chiave del router ed esistono due modi per creare una chiave. Il più semplice consiste nel consentire al software del router di convertire

una frase di accesso creata dall'utente in una chiave. Il metodo avanzato prevede l'inserimento manuale delle chiavi.

Server virtuali

Questa funzione consente di instradare eventuali richieste di servizio esterne (di Internet), tra cui le richieste di vari servizi tra cui quelli di server web (porta 80), server FTP (porta 21) o altre applicazioni attraverso il proprio router nella rete interna. Poiché i computer interni sono protetti da una protezione firewall, i computer di Internet non possono accedervi perché non li "vedono". Se fosse necessario configurare una funzione di server virtuale per una specifica applicazione, si dovrà contattare il fornitore dell'applicazione per conoscere le impostazioni delle porte necessarie.

Per digitare manualmente le impostazioni, inserire l'indirizzo IP nello spazio previsto per la macchina interna, il tipo di porta (TCP o UDP) e la(e) porta(e) pubbliche da superare. Quindi selezionare "Enable" (Abilita) e fare clic su "Set" (Imposta). È possibile passare soltanto attraverso una porta per ciascun indirizzo IP interno. L'apertura delle porte nella protezione firewall può comportare un rischio per la sicurezza. Le impostazioni possono essere attivate e disattivate molto rapidamente. È consigliabile disattivare le impostazioni quando non si utilizza un'applicazione specifica.

Filtri IP Client

Il router può essere configurato in modo da limitare l'accesso ad Internet, alla posta elettronica o ad altri servizi di rete in particolari giorni o momenti. La limitazione di accesso ai servizi può essere impostata per uno o più computer.

Il filtro indirizzi MAC

Il filtro indirizzi MAC è un potente mezzo per specificare quali sono i computer che possono accedere alla rete. Sarà negato l'accesso a qualsiasi computer che dovesse tentare di accedere alla rete e che non fosse specificato nell'elenco dei filtri. Attivando questa funzione, è necessario inserire l'indirizzo MAC per ciascun client nella propria rete per consentire l'accesso della rete ad ognuno oppure copiare l'indirizzo MAC selezionando il nome del computer dal "DHCP Client List" (Elenco Client DHCP). Per attivare questa funzione, selezionare "Enable" (Abilita). Quindi, fare clic su "Apply Changes" (Applica modifiche) per salvare.

DMZ

Se si ha un PC client che non è in grado di gestire adeguatamente un'applicazione Internet da dietro una protezione firewall, per il client è possibile aprire un accesso a Internet illimitato a due vie. Questa operazione

potrebbe essere necessaria qualora la funzione NAT entrasse in conflitto con un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Utilizzare questa funzione solo provvisoriamente. **Il computer nella DMZ non è protetto dagli attacchi degli hacker.**Per collocare il computer nella DMZ, digitare le ultime cifre del rispettivo indirizzo IP LAN nel campo "Static IP" (IP Statico) e fare clic su "Apply Changes" (Applica modifiche) affinché la modifica venga attivata.

Se si dispone di un unico indirizzo IP pubblico (WAN), l'IP pubblico può essere lasciato su "0.0.0.0". Se si stessero utilizzando diversi indirizzi pubblici (WAN) IP, è possibile selezionare a quale indirizzo pubblico (WAN) IP dirigere l'host DMZ. Digitare l'indirizzo pubblico (WAN) IP al quale si desidera indirizzare l'host DMZ, digitare le ultime due cifre dell'indirizzo IP del computer host DMZ e fare clic su "Apply Changes" (Applica modifiche).

Password Amministratore

Il router viene fornito SENZA password. Se si desidera aggiungere una password per maggiore sicurezza, la password può essere impostata dall'interfaccia utente basata sul server del router. Conservare la password in un posto sicuro, in quanto sarà necessaria per accedere al router in futuro. È anche **VIVAMENTE CONSIGLIATO** inserire una password nel caso si intenda utilizzare l'opzione di gestione a distanza. L'opzione di durata connessione consente di impostare un intervallo di tempo di connessione all'interfaccia avanzata di impostazione del router. Il timer parte dal momento in cui non si rileva alcuna attività. Ad esempio, se fosse stata apportata qualche modifica all'interfaccia di impostazione avanzata, il computer si gestirà da solo senza dover fare clic su "Logout".

Supponendo che la durata di connessione sia stata impostata su 10 minuti, dopo 10 minuti di mancato utilizzo del computer, la sessione di connessione verrà interrotta. Per apportare ulteriori modifiche sarà quindi necessario connettersi di nuovo al router. L'opzione di durata della connessione è prevista a scopo cautelativo ed è preimpostata su 10 minuti. Va ricordato che è possibile connettere all'interfaccia avanzata di impostazione del router soltanto un computer alla volta.

Orario e fuso orario

Il router aggiorna l'orario collegandosi ad un server SNTP (Simple Network Time Protocol). In questo modo il router è in grado di sincronizzare l'orologio del sistema con la rete Internet mondiale. L'orologio sincronizzato presente nel router viene utilizzato per registrare l'elenco di protezione e controllare il filtro client. Selezionare il proprio fuso orario. Se si vive in una zona che osserva l'ora legale, inserire un segno di spunta nella casella accanto a "Enable Daylight Saving" (Attiva ora legale). L'orologio del sistema potrebbe non aggiornarsi immediatamente. Attendere almeno 15 minuti perché il router contatti i server dell'orario su Internet e riceva una risposta.

Gestione a distanza

Prima di abilitare questa funzione, **ACCERTARSI DI AVER IMPOSTATO LA PASSWORD DELL'AMMINISTRATORE**. La gestione a distanza consente di modificare le impostazioni del router da qualsiasi punto di Internet.

UPnP

La tecnologia UPnP (Universal Plug-and-Play) è in grado di offrire un funzionamento continuo delle opzioni di trasmissione di messaggi vocali, video, giochi e di altre applicazioni conformi agli standard UPnP. Per funzionare correttamente, alcune applicazioni richiedono che la protezione firewall del router sia configurata in maniera specifica. In genere, questo richiede che si aprano le porte TCP e UDP e, in alcuni casi, che si impostino le porte trigger. Un'applicazione
conforme al servizio UPnP ha la capacità di comunicare con il router, fondamentalmente "dicendo" al router come configurare la protezione firewall. Il router viene fornito con l'opzione UPnP disabilitata. Se si sta utilizzando una qualsiasi applicazione conforme al servizio UPnP, e si desidera utilizzare le opzioni UPnP, queste si possono attivare. È sufficiente selezionare "Enable" (Abilita) nella sezione "UPnP Enabling" (Abilitazione UpnP) della pagina "Utilities" (Utility). Fare clic su "Apply Changes" (Applica modifiche) per salvare la modifica.

Allegato B: Considerazioni importanti per il posizionamento e l'installazione

Nota bene: Sebbene alcuni dei fattori elencati di seguito possano compromettere le prestazioni della rete, non ne impediscono il funzionamento. Se ritenete che la rete non funzioni efficientemente, la seguente lista di controllo potrebbe rivelarsi utile.

1. **Collocazione del router o dell'access point**

   Posizionare il router wireless (o l'access point), che rappresenta il punto di connessione centrale della rete, il più vicino possibile al centro della copertura dei dispositivi wireless.

   Per ottenere la migliore connessione per i "clienti wireless"(computer provvisti delle schede di rete wireless per notebook, schede di rete per computer desktop ed adattatori USB wireless Belkin):

   - Assicurarsi che le antenne di rete del router wireless o dell'access point siano parallele e verticali (rivolte verso il soffitto). Se il router wireless (o l'access point) è in posizione verticale, puntare le antenne il più possibile verso l'alto.
   - Negli edifici a più piani, posizionare il router wireless o l'access point su un piano che sia il più vicino possibile al centro dell'edificio. Ad esempio sul pavimento di un piano superiore.
   - Non mettere il router wireless o l'access point vicino a telefoni cordless da 2,4 GHz.

2. **Evitare ostacoli e interferenze**

   Evitare di posizionare il router wireless (o l'acces point) vicino a dispositivi che possono trasmettere "interferenze", come nel caso dei forni a microonde. Tra gli oggetti che possono impedire la comunicazione wireless sono compresi:

   - Frigoriferi
   - Lavatrici e/o asciugabiancheria
   - Armadietti in metallo
   - Acquari grandi
   - Finestre verniciate con vernice a base metallica di protezione dai raggi UV

Se il segnale wireless dovesse sembrare più debole in alcuni punti, assicurarsi che oggetti di questo tipo non ostacolino il segnale tra i computer e il router (o l'access point) wireless.

3. Telefoni cordless

Se le prestazioni della rete wireless dovessero continuare ad essere inadeguate, dopo aver verificato i punti sopra riportati, e se si ha un telefono cordless:

- allontanare il telefono cordless dal router wireless (o access point) e dai computer provvisti di tecnologia wireless;
- staccare la spina e rimuovere la batteria da eventuali telefoni cordless che utilizzano la banda 2,4 GHz (consultare le informazioni del produttore). Se il problema si risolve, la causa era probabilmente un'interferenza del telefono.
- se il telefono supporta la selezione dei canali, e se possibile, cambiare il canale sul telefono e scegliere il canale più lontano dalla rete wireless; Per esempio, spostare il telefono sul canale 1 e il Router Wireless (o Access Point) sull'11. Vedere il manuale utente per maggiori informazioni.
- Se necessario, passare ad un telefono cordless a 900 MHz o 5 GHz.

4. Scegliere il canale "più tranquillo" della propria rete wireless

Negli edifici dove sono presenti sia abitazioni che uffici, una rete vicina potrebbe entrare in conflitto con la vostra.

Usare le capacità Site Survey della utility LAN wireless del proprio adattatore wireless per localizzare eventuali reti wireless disponibili (vedere il manuale di istruzioni dell'adattatore wireless) e spostare il router wireless (o access point) ed i computer su un canale che sia il più lontano possibile da altre reti.

Provare con più canali, in modo da individuare la connessione più chiara ed evitare in questo modo interferenze da altri telefoni cordless o da altri dispositivi di rete wireless.

Per prodotti wireless Belkin, consultare l'opzione Site Survey e le informazioni sui canali wireless riportate nel manuale utente.

Queste indicazioni dovrebbero consentire di ottenere la migliore copertura possibile con il router wireless (o l'access point). Per coprire un'area più estesa, si consiglia di usare il Range Extender/Access Point Wireless Belkin.

1
2
3
4
5
6
7
8
9
10
sezione

5. Connessioni protette, VPN e AOL

Le connessioni protette generalmente richiedono un nome utente e una password e sono usate quando sono richieste condizioni di sicurezza. Le connessioni protette comprendono:

- Le connessioni Virtual Private Network (VPN), spesso usate per il collegamento remoto ad una rete di un ufficio
- Il programma di America Online (AOL) “Bring Your Own Access” , che permette di usare AOL mediante la banda larga fornita da un altro servizio via cavo o DSL
- La maggior parte dei siti web di home banking
- Molti siti commerciali che richiedono un nome utente e una password per accedere all’account

Le connessioni protette si possono interrompere configurando la gestione dell’alimentazione del computer, facendole “addormentare”. La soluzione più semplice per evitare che questo accada consiste nell’effettuare nuovamente il collegamento riavviando il software VPN o AOL o eseguendo di nuovo il login nel sito protetto.

Un’alternativa è cambiare le configurazioni della gestione dell’alimentazione del computer, in modo da non farlo addormentare; tuttavia, ciò potrebbe non essere raccomandabile per i portatili. Per modificare le configurazioni della gestione dell’alimentazione in Windows, vedere in “Opzioni risparmio energia” nel pannello di controllo.

Se le difficoltà con la connessione protetta VPN o AOL dovessero persistere, rivedere i passaggi nelle pagine precedenti per assicurarsi di aver individuato il problema.

Allegato C: Tabella delle impostazioni per la connessione a Internet

La tabella della pagina successiva fornisce alcuni valori di riferimento per selezionare e configurare la connessione Internet con la propria linea ADSL. Molti ISP utilizzano impostazioni diverse, a seconda della regione e dell’attrezzatura utilizzata. Si possono provare le impostazioni suggerite per gli ISP della propria regione, se non dovessero funzionare, rivolgersi al proprio ISP per ricevere i parametri specifici.

Nazione	Protocollo di connessione	VPI/VCI	Incapsulamento	ISP
Europa				
Francia	PPPoE	8/35	LLC	Vari
Germania	PPPoE	1/32	LLC	T-Online, vari
Olanda	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Vari
Belgio	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italia	PPPoE o PPPoA	8/35	VC MUX	TIN
Spagna	PPPoE oppure 1483 Bridged	8/32	LLC	Telefonica
Svezia	1483 Bridged	3/35	LLC	Telia
UK	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Asia				
Australia	PPPoE o PPPoA	8/35	LLC	Vari
Nuova Zelanda	PPPoE o PPPoA	0/100	VC MUX	Vari
Singapore	PPPoE	0/100	LLC	SingNet, Pacific Internet

Dichiarazione FCC

DICHIARAZIONE DI CONFORMITÀ ALLE NORMATIVE FCC PER LA COMPATIBILITÀ' ELETTROMAGNETICA

Noi sottoscritti, Belkin Corporation, con sede al 501 West Walnut Street, Compton, CA 90220, dichiariamo sotto la nostra piena responsabilità che il prodotto,

F5D9630-4

al quale questa dichiarazione fa riferimento, è conforme alla Parte 15 delle norme FCC. Le due condizioni fondamentali per il funzionamento sono le seguenti: (1) il dispositivo non deve causare interferenze dannose e (2) il dispositivo deve accettare qualsiasi interferenza ricevuta, comprese eventuali interferenze che possano causare un funzionamento anomalo.

Attenzione: esposizione alle radiazioni di radiofrequenza.
La potenza in uscita irradiata da questo dispositivo è molto inferiore ai limiti di esposizione alla radiofrequenza FCC. Tuttavia, il dispositivo dovrà essere utilizzato in modo da ridurre al minimo i potenziali rischi di contatto umano nel corso del suo funzionamento.

Se il dispositivo venisse collegato ad un'antenna esterna, l'antenna dovrà essere posizionata in modo da ridurre al minimo il potenziale rischio di contatto umano nel corso del suo funzionamento. Per evitare un eventuale superamento dei limiti di esposizione alle radiofrequenze FCC, non è consentito avvicinarsi all'antenna di oltre 20 cm nel corso del normale funzionamento.

Informazione della Commissione Federale per le Comunicazioni
Questa attrezzatura è stata testata ed è risultata conforme ai limiti previsti per le periferiche digitali di classe B, in conformità alla Sezione 15 delle normative FCC. Questi limiti hanno lo scopo di fornire una protezione ragionevole dalle interferenze dannose in un'installazione domestica.

Questo dispositivo genera, utilizza e può emettere energia in radiofrequenza. Se questo dispositivo causasse interferenze dannose per la ricezione delle trasmissioni radiotelevisive determinabili spegnendo o riaccendendo l'apparecchio stesso, si suggerisce all'utente di cercare di rimediare all'interferenza ricorrendo ad uno o più dei seguenti provvedimenti:

- Modificando la direzione o la posizione dell' antenna ricevente.
- Aumentando la distanza tra il dispositivo ed il ricevitore.
- Collegando il dispositivo ad una presa di un circuito diversa da quella cui è collegato il ricevitore.
- Rivolgendosi al rivenditore o ad un tecnico radio/TV specializzato.

Modifiche
Le indicazioni FCC prevedono che l'utente venga informato del fatto che eventuali variazioni o modifiche apportate a questo dispositivo non espressamente approvate da Belkin Corporation potrebbero annullare la facoltà dell'utente di utilizzare il dispositivo.

Canada-Industry Canada (IC)
L'apparecchio radio wireless di questo dispositivo è conforme alle indicazioni RSS 139 & RSS 210 Industry Canada. Questo apparecchio digitale di Classe B è conforme allo standard canadese ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Europa -Comunicato dell'Unione Europea
CE 0560 ⓘ
I prodotti radio con la sigla di avvertenza CE 0560 o CE sono conformi alla direttiva R&TTE (1995/5/EC) emessa dalla Commissione della Comunità Europea..

La conformità a tale direttiva implica la conformità alle seguenti norme europee (tra parentesi sono indicati i rispettivi standard internazionali).

CE ⓘ

- EN 60950 (IEC60950) – Sicurezza del prodotto
- EN 300 328 Esigenze tecniche per i dispositivi radio
- ETS 300 826 - Esigenze generali EMC per dispositivi radio

Per stabilire il tipo di trasmettitore utilizzato, verificare la targhetta di identificazione del proprio prodotto Belkin.

I prodotti con il marchio CE sono conformi alla Direttiva sulla compatibilità elettromagnetica (89/336/CEE) e alla Direttiva per la Bassa Tensione (72/23/CEE) emesse dalla Commissione della Comunità Europea. La conformità a tale direttiva implica la conformità alle seguenti norme europee (tra parentesi sono indicati i rispettivi standard internazionali).

CE

- EN 55022 (CISPR 22) – Interferenze elettromagnetiche
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Immunità elettromagnetica
- EN 61000-3-2 (IEC610000-3-2) – Armoniche della linea di alimentazione
- EN 61000-3-3 (IEC610000) – Sfarfallio della linea di alimentazione
- EN 60950 (IEC60950) - Sicurezza del prodotto

I prodotti che contengono un trasmettitore radio presentano le etichette di avvertimento CE 0560 o CE, e possono anche esibire il logotipo CE.



Questo simbolo posto sul prodotto o sulla sua confezione indica che tale prodotto non deve essere gettato via insieme ai rifiuti domestici. L'utente ha la responsabilità di liberarsi dell'apparecchiatura portandola in un punto di raccolta deputato al riciclaggio di rifiuti di apparecchi elettrici ed elettronici. La raccolta separata e il riciclaggio degli apparecchi da smaltire contribuiranno alla salvaguardia delle risorse naturali e garantiranno che il prodotto sia riciclato in modo da non mettere in pericolo la salute umana. Per maggiori informazioni sui punti di smaltimento e riciclaggio per le apparecchiature elettroniche, vi preghiamo di contattare il vostro comune, il servizio di smaltimento rifiuti domestici o il negozio in cui avete acquistato.

Prodotto garantito a vita da Belkin Corporation Limited

Belkin Corporation garantisce a vita questo prodotto da eventuali difetti di materiale e lavorazione. Qualora venisse rilevata un'anomalia, Belkin provvederà, a propria discrezione, a riparare o sostituire il prodotto gratuitamente, a condizione che esso sia restituito entro il periodo di garanzia, con le spese di trasporto prepagate, al rivenditore Belkin autorizzato da cui è stato acquistato. Potrebbe venire richiesta la prova di acquisto.

Questa garanzia non sarà valida nel caso il prodotto sia stato danneggiato accidentalmente, per abuso, uso non corretto o non conforme, qualora sia stato modificato senza il permesso scritto di Belkin, o nel caso il numero di serie Belkin fosse stato cancellato o reso illeggibile.

LA GARANZIA E I RIMEDI DI CUI SOPRA PREVALGONO SU QUALSIASI ALTRO ACCORDO, SIA ESSO ORALE, SCRITTO, ESPRESSO O IMPLICITO. BELKIN DECLINA SPECIFICATAMENTE QUALSIASI OBBLIGO DI GARANZIA IMPLICITO COMPRESE, SENZA LIMITI, LE GARANZIE DI COMMERCIABILITÀ O IDONEITÀ AD UN PARTICOLARE SCOPO.

Nessun rivenditore, agente o impiegato di Belkin è autorizzato ad apportare modifiche, ampliamenti o aggiunte alla presente garanzia.

BELKIN DECLINA QUALSIASI RESPONSABILITÀ PER EVENTUALI DANNI SPECIALI, ACCIDENTALI, DIRETTI O INDIRETTI IMPUTABILI AD UN'EVENTUALE VIOLAZIONE DELLA GARANZIA O IN BASE A QUALSIASI ALTRA TEORIA LEGALE, COMPRESI, MA NON SOLO, I CASI DI MANCATO GUADAGNO, INATTIVITÀ, DANNI O RIPROGRAMMAZIONE O RIPRODUZIONE DI PROGRAMMI O DATI MEMORIZZATI O UTILIZZATI CON I PRODOTTI BELKIN."

Poiché alcuni Stati non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, i limiti di esclusione di cui sopra potrebbero non fare al caso vostro. Questa garanzia consente di godere di diritti legali specifici ed eventuali altri diritti che possono variare di stato in stato.

BELKIN®

Modem ADSL2+ con router G+ MIMO wireless

Per maggiori informazioni sull'assistenza tecnica, visitare il nostro sito web www.belkin.it nell'area Centro assistenza.
"Per contattare telefonicamente il servizio di assistenza tecnica, chiamare uno dei seguenti numeri*. L'assistenza tecnica è disponibile 24 ore su 24, 7 giorni su 7".

*Si applicano solo le tariffe delle chiamate locali

Assistenza tecnica gratuita*

AUSTRIA	08 - 20 20 07 66	LUSSEMBURGO	34 20 80 8560
REPUBBLICA CECA	23 900 04 06	PAESI BASSI	0900 - 040 07 90
DANIMARCA	701 22 403	NORVEGIA	815 00 287
FINLANDIA	00800 - 22 35 54 60	POLONIA	00800 - 441 17 37
FRANCIA	08 - 25 54 00 26	PORTOGALLO	707 200 676
GERMANIA	0180 - 500 57 09	RUSSIA	495 580 9541
GRECIA	00800 - 44 14 23 90	SUDAFRICA	0800 - 99 15 21
UNGHERIA	06 - 17 77 49 06	SPAGNA	902 - 02 43 66
ISLANDA	800 8534	SVEZIA	07 - 71 40 04 53
IRLANDA	0818 55 50 06	SVIZZERA	08 - 48 00 02 19
ITALIA	02 - 69 43 02 51	REGNO UNITO	0845 - 607 77 87

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
7 Bowen Crescent, West Gosford
NSW 2250, Australia
+61 (0) 2 4372 8600
+61 (0) 2 4372 8603 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Regno Unito
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Paesi Bassi
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

P75125ea_A